Symantec Brightmail AntiSpam™

Version 6.0

Installation Guide

Copyright © 2004-2005 Symantec Corporation and/or its subsidiaries. All rights reserved.

Symantec Brightmail AntiSpam™
Version 6.0.2
Installation Guide
Document Version 1.0

Brightmail, the Brightmail logo, BLOC, BrightSig, Probe Network and The Anti-Spam Leader are trademarks or registered trademarks of Symantec Corporation.

Symantec and the Symantec logo are U.S. registered trademarks and Symantec Security Response (SSR) is a trademark of Symantec Corporation.

Symantec Brightmail AntiSpam is protected under U.S. Patent No. 6,052,709.

Microsoft, Windows, and/or other Microsoft products referenced herein are either trademarks or registered trademarks of Microsoft.

For third party notices, see Appendix B, “Third Party Licenses,” on page 145.

All other trademarks, service marks, trade names, or company names referenced herein are used for identification only and are the property of their respective owners.

Symantec Corporation
20330 Stevens Creek Blvd.
Cupertino, CA 95014
U.S.A.
Voice +1 408 517 8000
http://www.symantec.com

Table of Contents

Symantec Brightmail AntiSpam Overview 1
- What's New in Symantec Brightmail AntiSpam 2
- Symantec Brightmail AntiSpam Architecture Overview 3
  - Brightmail Scanner 4
  - Brightmail Control Center 5
- Group Policies, Email Categories, and Filtering Actions 6
- Brightmail Filters 8
  - AntiSpam Filters 8
  - Content Filters 9
  - Blocked and Allowed Senders Lists 9
  - AntiVirus Filters 10
- Brightmail Conduit 11
- Brightmail Quarantine 11
- Spam Foldering and Submissions 11
- Installation Sequence 12

Installing Brightmail Scanner for Sendmail 15
- Preparing to Install Brightmail Scanner 15
  - Confirm Hardware Requirements 15
  - Confirm Software and Location Requirements 16
  - Enable Sendmail External Filtering 17
  - Create Required Accounts and Directories 18
- Installing Brightmail Scanner for Sendmail 19
  - Find and Run the Install Script 19
  - Upgrading Software 21
  - Installing with the Command-Line Installer 23
  - Starting a Brightmail Scanner 30
  - Registering to Receive New AntiSpam Filters 30
- What to Do Next 31

Uninstalling Brightmail Scanner for Sendmail 31
Uninstalling with the Command-Line Installer 31

Configuring Sendmail for the Brightmail Filter 33
Understanding the Filter Address and Optional Settings 33
Configuring Sendmail Switch to Work with Brightmail Scanner 35
Configuring Sendmail for Brightmail Scanner with sendmail.cf 40
Configuring Sendmail for Brightmail Scanner with M4 41

Installing Brightmail Scanner for Windows 43
Hardware Requirements 43
Software Environment 43
Upgrading Software 44
Installing Brightmail Scanner for Windows 46
Verifying Brightmail Scanner Installation 53
Modifying, Repairing, and Removing Brightmail Scanner 54

Installing Brightmail Control Center 57
Hardware Requirements 57
Software Environment Requirements 58
Operating System Compatibility 58
LDAP Compatibility for Brightmail Quarantine 59
Web Browser Compatibility 59
Checking for Port Availability Via TCP/IP 60
Upgrading Software 60
Installing Brightmail Control Center on UNIX 60
Accessing the UNIX Install Script 61
Running the Installer on UNIX 62
Reinstalling Control Center on UNIX 67
Installing Brightmail Control Center on Windows 67
Automatic Startup Configured by Brightmail Control Center Installer 73
Uninstalling Brightmail Control Center on UNIX 73
Uninstalling Brightmail Control Center on Windows 73

Control Center Testing and Configuration 75
Testing Installation of the Brightmail Control Center 76
Reviewing the Installation Log 76
Logging in and Logging out 76
Checking Versions 76
Adding a Brightmail Scanner 77
Starting a Brightmail Scanner from the Brightmail Control Center . . 78

Testing Symantec Brightmail AntiSpam Filtering 78
Verifying Normal Delivery 78
Verifying Spam Filtering 79
Testing AntiVirus Filtering 79
Verifying Spam Filtering to Quarantine 79
Configuring the Brightmail Control Center to Use WebLogic 81
Copying the MySQL Connector/J API 81
Adding MySQL Connector/J to the CLASSPATH Variable 81
Configuring the Brightmail JDBC Connection Pool 82
Configuring a Data Source 85
Deploying the brightmail.war 86
Testing the Control Center with the WebLogic Application Server . . 86

Plug-Ins and Foldering 87
Installing the Symantec Plug-in for Outlook 87
Usage Scenarios 87
End User Experience 88
Software Requirements 89
Administrator Setup Instructions 89
Configuring Automatic Spam Foldering 93
Configuring the Spam Folder Agent 93
Configuring the Symantec Spam Folder Agent for Domino 95
Enabling Automatic Spam Foldering 105

Appendix A: Symantec Brightmail AntiSpam Files 107
Brightmail Scanner on UNIX 108
Brightmail Scanner, Complete (Brightmail Server, Brightmail Client) 108
Brightmail Scanner Installation with Brightmail Server Only 113
Brightmail Scanner Installation with Brightmail Client Only 118
Brightmail Scanner on Windows 120
Brightmail Scanner, Complete (Brightmail Server, Brightmail Client) 120
Brightmail Scanner Installation with Brightmail Server Only 127
Brightmail Scanner Installation with Brightmail Client Only 132
Brightmail Control Center on All Platforms 134

Appendix B: Third Party Licenses 145

Index 151

Symantec Brightmail AntiSpam Overview

Welcome to Symantec Brightmail AntiSpam™, Symantec's industry-leading message filtering system. Symantec Brightmail AntiSpam offers complete, Internet-wide, server-side antispam and antivirus protection. It actively seeks out, identifies, analyzes, and ultimately defuses spam and virus attacks before they inconvenience your users and overwhelm or damage your networks. Symantec software allows you to remove unwanted mail before it reaches your users' inboxes, without violating their privacy.

Symantec Brightmail AntiSpam software filters email in four ways:

- AntiSpam Filters use our state-of-the-art technologies and strategies to filter and classify email as it enters your site.
- AntiVirus Filters combine Symantec processing technology with Symantec AntiVirus definitions and engines to clean viruses from your email.
- Content Filters supplement AntiSpam Filters; you can tailor them specifically to the needs of your organization.
- The Allowed Senders List and the Blocked Senders List filter messages based on the sender. You can create your own lists and subscribe to third-party lists. Symantec Brightmail AntiSpam includes the Brightmail Reputation Service, which consists of our Open Proxy List, Safe List and Suspect List. These features filter messages based on extensive research to ascertain the reputation of the originating IP address, as a source of spam or of legitimate email.

This section contains the following topics:

- What's New in Symantec Brightmail AntiSpam
- Symantec Brightmail AntiSpam Architecture Overview
- Group Policies, Email Categories, and Filtering Actions
- Brightmail Filters
- Brightmail Conduit
- Brightmail Quarantine
- Spam Foldering and Submissions
- Installation Sequence

What's New in Symantec Brightmail AntiSpam

Symantec Brightmail AntiSpam Version 6.0 provides the following enhancements over previous releases:

Table 1. Symantec Brightmail AntiSpam Version 6.0 Enhancements

Feature	Description
Brightmail Control Center	The Brightmail Control Center (Control Center) is a Web-based cross-platform configuration and administration center built in Java. Each Symantec Brightmail AntiSpam installation has one Control Center, which also houses Brightmail Quarantine and supporting software. You can configure and monitor all of your Brightmail Scanners from the Control Center. The Control Center replaces the Brightmail configuration file, the Configurator and the Brightmail Administration Console. These components are no longer included in Symantec Brightmail AntiSpam.
Brightmail Scanner	Brightmail Scanners perform email filtering. Your Symantec Brightmail AntiSpam installation can have one or many Brightmail Scanners. Each Brightmail Scanner includes one or both of the following components: Brightmail Server, Brightmail Client.
Multiple-Machine Management	You can now configure and manage multiple Brightmail Scanners from one Brightmail Control Center. Previously each computer filtering email had to be configured individually.
Group Policies	You can now specify an unlimited number of user groups, identified by email addresses or domain names, and customize mail filtering for each group.
Improved Filtering	Numerous improvements have been made to Symantec Brightmail AntiSpam's filtering technologies, including enhanced effectiveness for URL Filters and Heuristic Filters; filtering on mailto: links in messages; improved filtering on MIME headers; and the next generation of Signature Filters, which target comparisons to specific message components with surgical precision.
Brightmail Reputation Service	The Brightmail Reputation Service provides comprehensive reputation tracking that enhances the power of Symantec Brightmail AntiSpam. Symantec manages three lists as part of the Brightmail Reputation Service. Each list operates automatically and filters your messages using the same technology as Symantec's other filters. The Brightmail Reputation Service includes the Open Proxy List, the Safe List and the Suspect List.
Improved Reporting	For added convenience and clarity, pre-set reports are now separated into two groups: antispam reports and antivirus reports. You can choose from a selection of reports; each report can be customized to include specific date ranges, time period groupings, and various delivery and output options. For some reports, you can filter based on specific recipients and senders of interest.
Language Identification	Users of the Brightmail Plug-in for Outlook can choose from a list of languages in which they would like to receive messages. Messages identified as written in a language not on the user's list will be filtered as spam.
Quarantine Management and End User Improvements	Brightmail Quarantine is now managed via the Brightmail Control Center. You can now set messages to be deleted based on the total size of the Quarantine database or based on each user's storage usage. When users receive digest notifications from Brightmail Quarantine, they can now click on a View link to view an individual message, or click on a Release link to release a message back to the inbox.

Symantec Brightmail AntiSpam Architecture Overview

Using Brightmail AntiSpam, you set up a powerful message filtering system that protects your customers and your network through an approach that is centralized and automated, but also provides customizable, open features that you can tailor for your system. The net effect of this highly scalable structure is to unburden your customers of unwanted email.

As spam messages traverse the Internet, they pass through Symantec's worldwide Probe Network™, an extensive array of email addresses. The Probe Network includes over two million probe accounts that attract the latest spam, based upon up-to-date research into spamming methodologies. The Probe Network sends possible spam emails in real time to the Brightmail Logistics and Operations Center (BLOC™) for evaluation. If the message is verified as spam, the BLOC issues AntiSpam Filters to Brightmail Scanners on your system that isolate similar messages.

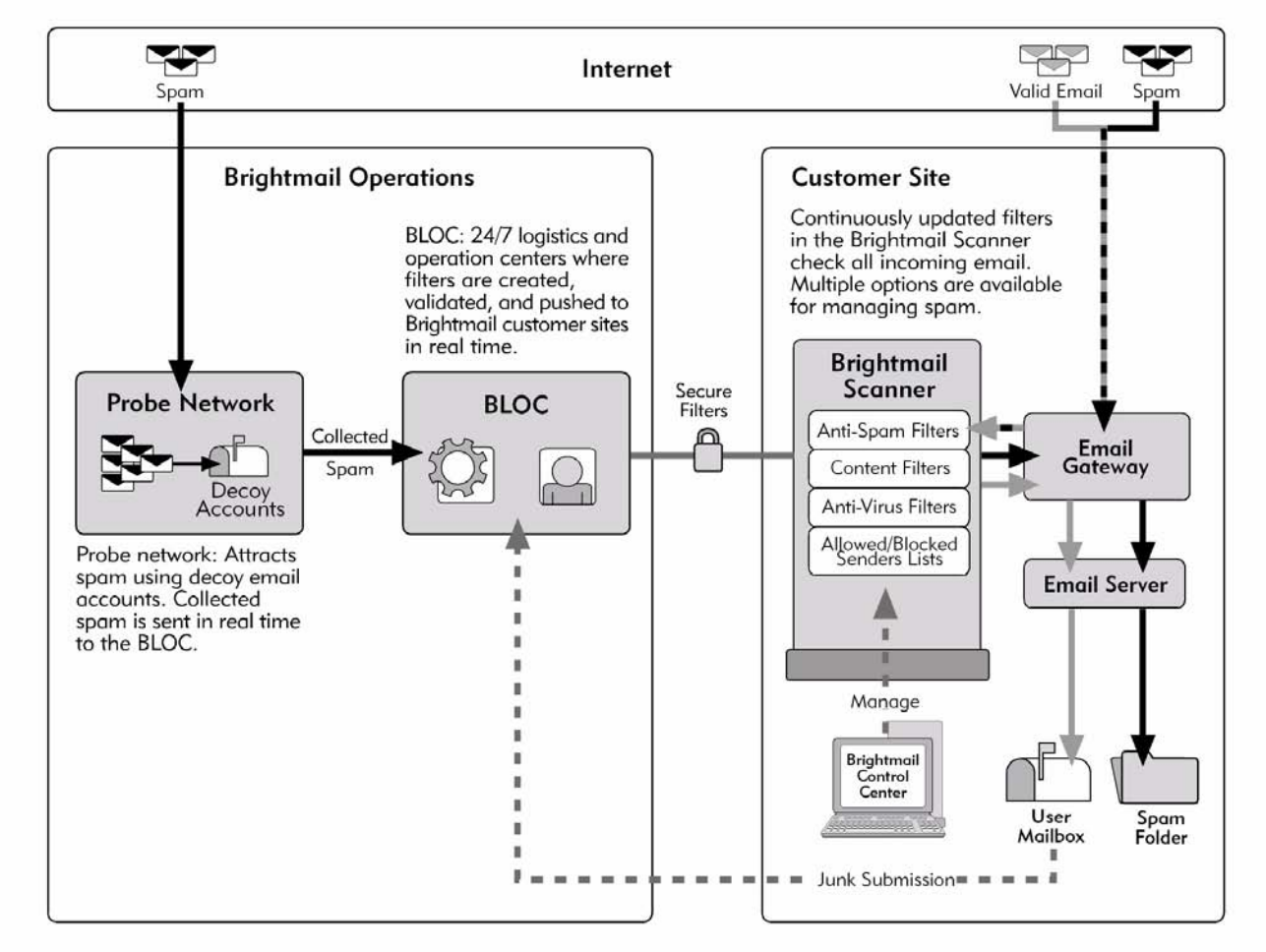
The BLOC consists of several centers working cooperatively on three continents, comprising a round-the-clock protection network that spans the globe. Sophisticated automatic tools, assisted and monitored by BLOC Technicians, evaluate mail for new variations of spam, then issue filters to identify and capture similar messages. The BLOC continuously provides updated filters to Brightmail Servers on your system. BLOC Technicians play an important role in confirming the identification of possible spam. This combination of automation and human intervention allows Symantec Brightmail AntiSpam to adapt in real time to ever-changing spamming techniques, giving it unparalleled flexibility and accuracy as a spam filter.

Most of the filters that the BLOC creates are designed to thwart specific spam attacks. A spam attack can contain thousands of identical or similar messages. By targeting filters against specific attacks, the BLOC keeps Symantec's false positive rate extremely low (less than 1 in 1 million).

Symantec also employs a carefully designed set of heuristic filters, which target patterns common in spam and add a proactive element to our spam-fighting arsenal. Commonly available heuristic filters can lead to large increases in false positives because of the problems inherent in a pattern-matching approach. Symantec Brightmail AntiSpam heuristic filters are carefully designed and tested to prevent large increases in false positives.

Figure 1 shows an overview of Symantec Brightmail AntiSpam.

Figure 1. Symantec Brightmail AntiSpam Overview



Brightmail Scanner

Each installation of Symantec Brightmail AntiSpam can have one or more Brightmail Scanners. Brightmail Scanners perform the actual filtering of email messages.

Each Brightmail Scanner contains:

- A Brightmail Agent
- One or both of the following:
  - A Brightmail Server
  - A Brightmail Client. If the Brightmail Scanner contains a Brightmail Client, then a supported mail transfer agent (MTA) must also reside on the same computer.

Brightmail Agent

This component communicates with the Brightmail Control Center to support centralized configuration and administration activities.

Brightmail Client

The Brightmail Client is a communications channel between the MTA and the Brightmail Server. You can use multiple Brightmail Clients; each one can talk to multiple Brightmail Servers. The Brightmail Client performs load balancing between Brightmail Servers.

Brightmail Server

The Brightmail Servers at your site process spam based on configuration options you select. Each Brightmail Server is a multi-threaded process that listens for requests from Brightmail Clients. Using a variety of state-of-the-art technologies, the Brightmail Server filters messages for classification. The classification, or verdict, is then returned to the Brightmail Client for subsequent delivery action.

Brightmail Control Center

Each Symantec Brightmail AntiSpam installation has exactly one Brightmail Control Center. This is the central nervous system of your Symantec software. The Brightmail Control Center communicates with the Brightmail Agent on each of your Brightmail Scanners. For smaller installations, you can install the Brightmail Control Center and the Brightmail Scanner on the same computer.

From this Web-based graphical user interface, you can:

- Configure, start and stop each of your Brightmail Scanners.
- Specify email filtering options for groups of users or for all of your users at once.
- Monitor consolidated reports and logs for all Brightmail Scanners.
- See summary information.
- Administer Brightmail Quarantine.
- View online help for Brightmail Control Center screens.

The Brightmail Control Center contains the following software:

Brightmail Quarantine

Brightmail Quarantine provides storage of spam messages and Web-based end user access to spam. You can also configure Brightmail Quarantine for administrator-only access. Use of Brightmail Quarantine is optional.

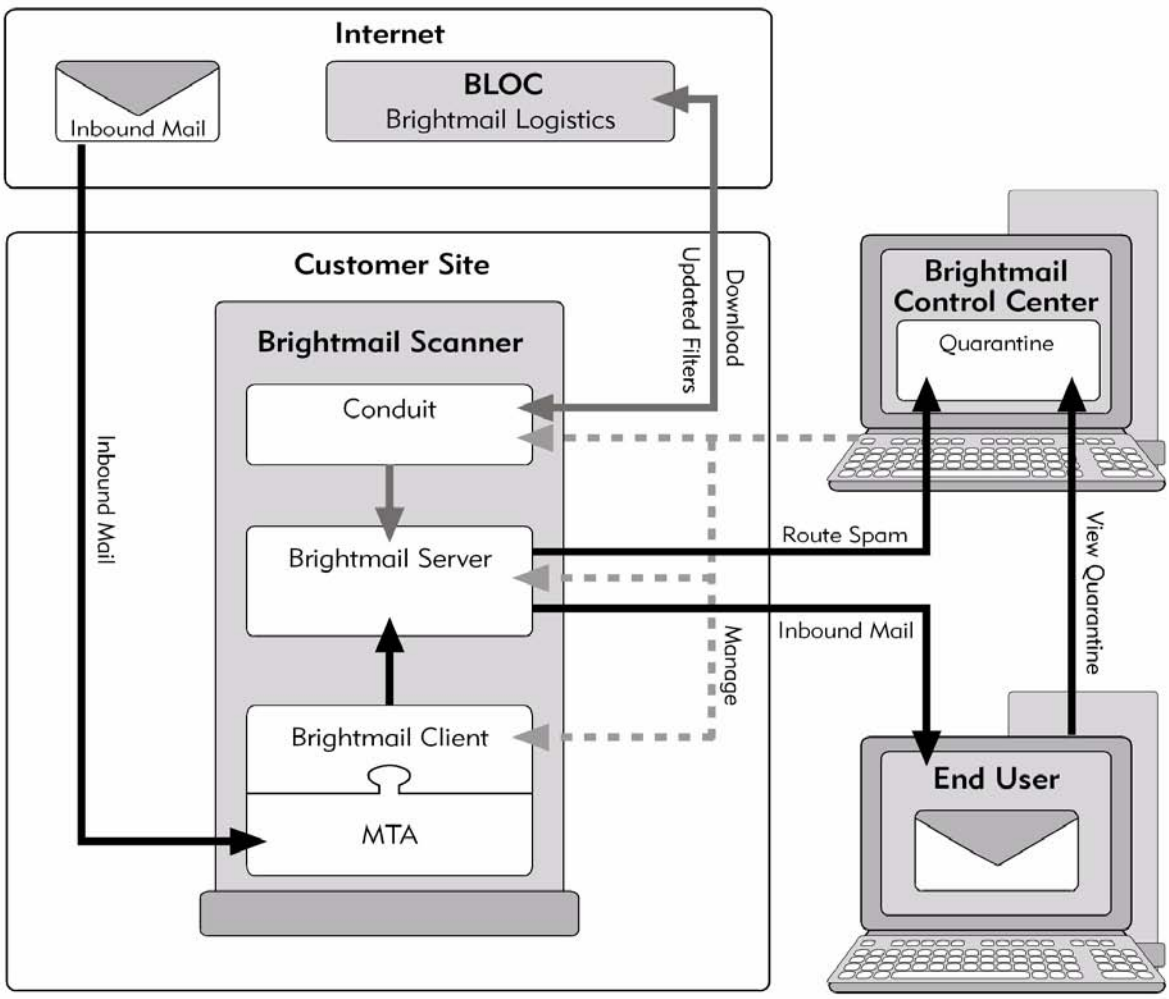
Third Party Software: Database, Web Server

A single MySQL database stores all of your Symantec Brightmail AntiSpam configuration information, as well as Brightmail Quarantine information and emails (if you are using Brightmail Quarantine). Configuration information is communicated to each Brightmail Scanner via an XML file. A Java-based Web Server (by default this is the Tomcat Web

Server) performs Web hosting functions for the Brightmail Control Center and Brightmail Quarantine.

Figure 2 shows the major components of Symantec Brightmail AntiSpam installed at your site.

Figure 2. Symantec Brightmail AntiSpam Components



Group Policies, Email Categories, and Filtering Actions

Symantec Brightmail AntiSpam provides a wide variety of actions for filtering email, and allows you to either set identical options for all users, or specify different actions for different groups of users.

You can specify groups of users based on email addresses or domain names. For each group, you can specify email filtering actions for seven different categories of email. For each category you can specify one of up to eight different filtering options.

You can choose different filtering actions for the following categories of email:

- **Spam –** Email messages identified as spam using Symantec's AntiSpam Filters.
- **Suspected spam –** You can use Symantec's Spam Scoring to identify a range of email as suspected spam, based on scores assigned by AntiSpam Filters.
- **Email from blocked senders –** You can specify a list of blocked senders, and you can use third party blocked senders lists. The lists included in the Brightmail Reputation Service are used by default.
- **Emails infected with viruses –** Symantec identifies virus-infected emails using AntiVirus Filters, based on Symantec virus definitions and engines.
- **Mass-mailing worms –** Symantec Brightmail AntiSpam identifies mass-mailing worm emails as distinct from spam or virus emails, because many customers prefer to delete these emails immediately.
- **Unscannable emails –** These are emails that could not be scanned due to size restrictions or other variables. They may or may not contain viruses. You can choose how to handle these messages.
- **Custom filtered emails –** You can specify special filters unique to your organization, to filter for specific content in email messages.

In addition to the seven categories listed above, you can also specify trusted senders by creating an Allowed Senders List and by subscribing to third party allowed senders lists. Messages from allowed senders are automatically sent to user inboxes, bypassing all filtering (except antivirus filtering, if enabled). The Safe List, part of the Brightmail Reputation Service, is implemented by default.

The filtering actions available vary by email category, and include the following:

- Deliver messages normally.
- Mark messages as spam, either by altering the subject line or by including a configurable X-Header.
- Delete messages.
- Route messages to an administrator's mailbox for subsequent examination.
- Save messages in a directory specified for that purpose.
- Send messages to Brightmail Quarantine, where users can access them via the Web.
- Route messages to each user's spam folder using the Spam Folder Agent, native foldering in Exchange 2003, or the Symantec Spam Folder Agent for Domino.
- Clean messages of viruses and deliver each cleaned message normally, with a notification to the recipient.

Brightmail Filters

Symantec Brightmail AntiSpam employs the following four major types of filters:

- **AntiSpam Filters –** AntiSpam Filters are created by Symantec using our state-of-the-art technologies and strategies to filter and classify email as it enters your site.
- **Content Filters –** Custom content filters are written by you, using the Brightmail Control Center or the Sieve scripting language, to tailor filtering to the needs of your organization.
- **Blocked and Allowed Senders Lists –** You can create lists of blocked senders and allowed senders and you can use third party lists. The lists included in the Brightmail Reputation Service are deployed by default.
- **AntiVirus Filters –** Antivirus definitions and engines provided by Symantec protect your users from email-borne viruses.

AntiSpam Filters

The nature of spam—and the business implications of false positives—demands a careful and flexible approach to filter creation. Accordingly, Symantec does not use a one-size-fits-all approach to creating filters. Instead, it employs a combination of filtering strategies, based on the specific type of spam. Some technologies perform sophisticated comparisons with the latest spam received by the Probe Network, resulting in matches of unparalleled accuracy. Others are more proactive, attacking future spam based on special characteristics or origination information. Symantec filter types include:

- Heuristic Filters
- URL Filters
- Signature Filters
- Header Filters

Heuristic Filters – Heuristic Filters scan the headers and the body of a message, applying a variety of tests. These tests search for tell-tale characteristics that are usually inherent in spam, such as opt-out links, specific phrases, and forged headers. Each characteristic is assigned a spam probability, and the message is given a cumulative probability score based on the overall test results. If a certain probability threshold is reached, Symantec Brightmail AntiSpam determines the message to be spam. Using heuristics, Symantec Brightmail AntiSpam software can make the determination that a message is spam, even if it hasn't passed through the Probe Network. The BLOC transmits updated Heuristic Filters as it does other AntiSpam Filters.

URL Filters – Symantec's URL Filters catch messages based on specific URLs found in spam. URL-based spam is increasingly pervasive because spammers want to direct readers to a specific Web site for contact information or purchasing instructions. Although the underlying URLs do not change frequently, spammers attempt to obfuscate and disguise them. As a result, these URLs appear to be unique across similar spam messages.

Signature Filters – When messages flow into the BLOC, they are characterized using proprietary algorithms into a unique *signature*, which is added to the database of known spam. Using this signature, Signature Filters group and match seemingly random messages that originated from a single attack. By distilling a complex and evolving attack to its DNA, more spam can be deflected with a single filter. Signature Filters include BrightSig2 Filters, Body Hash Filters and Attachment Filters.

Header Filters – Header Filters are regular expression-based filters that are applied to the header lines of a message. Header Filters can be used to compare email messages to spam messages seen by the Probe Network, and to exploit commonalities or trends present in spam messages (similar to the use of Symantec's Heuristic Filters).

Content Filters

You can create custom content filters, using either the Custom Filters Editor provided through the Brightmail Control Center, or using a Sieve filters file. You can specify a wide variety of filtering criteria. You have three sets of choices for the action to take on these messages:

- Deliver normally.
- Treat the same as another email category: you can use the same action on custom-filtered messages that you chose for spam, viruses, or any other category.
- Treat as company-specific content: choose a unique action for custom-filtered messages.

Blocked and Allowed Senders Lists

You can use lists of blocked and allowed senders (also known as *blacklists* and *whitelists*) in a variety of ways:

- **Define a custom Allowed Senders List –** Allowed senders are approved or trusted senders. Unless AntiVirus Filters detect a virus or worm, Symantec Brightmail AntiSpam treats mail coming from an address or connection in your Allowed Senders List as legitimate mail. Such mail is delivered immediately to the inbox, bypassing any other filtering. You therefore cannot choose message handling actions for messages from allowed senders; by definition these messages will be delivered to the user inbox.
- **Define a custom Blocked Senders List –** You can block messages from any senders you wish. You can define message handling actions that apply to messages from blocked senders for each group policy.
- **Check incoming mail against third party blocked senders lists and third party allowed senders lists –** Third parties compile and manage lists of desirable or undesirable domains, IP connections, and networks. A *DNS blacklist* is a common example of such a list. DNS blacklists allow subscribers to check, using DNS lookups, whether incoming mail is originating from known spammers. Many of the hosts on the list typically are running open SMTP relays or open proxy server ports. Such insecure relays and ports are effective conduits for sending unsolicited bulk email. Subscribers

to DNS lists can thus block or delete mail from these blacklisted hosts. On the other hand, administrators who subscribe to *DNS whitelists* can leverage a list of legitimate mail servers and senders. You can add a DNS blacklist as a third-party blocked senders list. You can add a DNS whitelist as a third party allowed senders list.

— **Brightmail Reputation Service Lists:** By default, Symantec Brightmail AntiSpam is configured to check mail against three lists, all part of the Brightmail Reputation Service, managed by Symantec. Unlike other lists, which simply aggregate information and are frequently outdated, the Brightmail Reputation Service lists are generated and updated hourly. They are downloaded to your system and updated just like other filters.

  – The **Open Proxy List** is a dynamic database containing IP addresses of identity-masking relays, including proxy servers with open or insecure ports. Because open proxy servers allow spammers to conceal their identities and off-load the cost of emailing to other parties, spammers will continually misuse a vulnerable server until it is brought offline or secured. Symantec recommends that organizations secure their proxy servers to ensure that spammers cannot connect to open ports and relay SMTP email.

  – The **Safe List** is a list of IP addresses from which virtually no outgoing email is spam.

  – The **Suspect List** is a list of IP addresses from which virtually all outgoing email is spam.

AntiVirus Filters

NOTE: *The following information and all other references to antivirus functions assume you have purchased antivirus filtering.*

Virus experts at Symantec Security Response (SSR) provide up-to-date virus definitions and engines to rid email attachments of viruses.

The BLOC—through automated processes monitored by BLOC Technicians—integrates the virus definitions and engines into AntiVirus Filters, tests them, and distributes them to your site.

The Brightmail Scanner—using the AntiVirus Cleaner (Cleaner)—filters the attachments of incoming email in search of viruses. If filtering detects no viruses, the message is analyzed for spam. If filtering detects one or more viruses, the policies you have set up go into effect. For example, you can instruct the Brightmail Scanner to delete the message or to clean and then deliver the message. You can also set policies potential virus messages that cannot be processed by the Cleaner.

Symantec Brightmail AntiSpam also provides protection against mass-mailing worms, which can leave hundreds of spam messages in their wake. The Worm Auto-Delete feature automatically removes not only the worm but also the associated emails. This convenient feature saves users from having to wade through hundreds of inbox messages that, although clean from viruses, server no valuable purpose.

The Cleaner creates a configurable advisory text message. This message informs the user that the infected attachment has been cleaned, deleted, or delivered without cleaning. The Cleaner inserts the original message, if delivered, as an attachment to the advisory message. The Cleaner also places a special identifying line in the message header so that the message is not filtered again for viruses.

Brightmail Conduit

Having up-to-date filters is imperative to ensure the highest success rate of filtering and blocking unwanted email. Filter updates are accomplished through a dialogue between the BLOC and the Brightmail Conduit, a component that runs at your site. The Conduit handles all such communication at your site. The Conduit runs on each Brightmail Scanner that contains a Brightmail Server.

The Conduit polls a secure Web site every minute to check for the availability of new filters from the BLOC. If new filters are available, the Conduit retrieves the updated filters using secure HTTPS file transfer. After authenticating the filters, the Conduit notifies the Brightmail Server to begin using the updated filters. The Conduit also manages statistics, both for use by the BLOC and by the Brightmail Control Center, which aggregates the statistics from Brightmail Scanners to create consolidated reports.

Brightmail Quarantine

Brightmail Quarantine (Quarantine) provides users direct Web-based access to spam messages that Symantec software has sidelined into the Quarantine database for them. Users can check for misidentified messages, resend messages to their inbox, and delete or search messages. An administrator account provides access to all quarantined messages.

Quarantine stores spam messages in the Symantec Brightmail AntiSpam MySQL database on the Brightmail Control Center computer. A Notifier process periodically sends users a reminder to check their spam messages in Quarantine. Spam messages older than a customizable time period are deleted automatically by an Expunger process. A Java-based Web Server presents the Quarantine interface to users.

Spam Foldering and Submissions

Symantec Brightmail AntiSpam features the Spam Folder Agent and the Symantec Spam Folder Agent for Domino, designed to work on Microsoft Exchange and Lotus Domino Servers, respectively. Installed separately from the standard Brightmail installation, these agents create a subfolder and a server-side filter in each user’s mailbox. This filter gets applied to messages that the Brightmail Scanner identifies as spam, routing spam into each user’s spam folder. The spam folder agents relieve end users and administrators of the burden of using their mail clients to create filters. The Symantec Spam Folder Agent for Domino also allows users to submit missed spam and false positives to Symantec.

The Symantec Plug-in for Outlook makes it easy for Outlook users to submit missed spam and false positives to Symantec. Depending on how you configure the plug-in, user submissions can also be sent automatically to a local system administrator. The Symantec Plug-in for Outlook also gives users the option to administer their own allowed senders and blocked senders lists.

Refer to "Plug-Ins and Foldering," on page 87 for more information about spam foldering options and submissions.

Installation Sequence

Different environments and circumstances may influence how you approach installation. This document presents a basic approach that is applicable in a variety of circumstances and works for many, if not most, enterprise installations. As always, we welcome your feedback on the procedure.

To install Symantec Brightmail AntiSpam:

1. Verify your software, hardware and operating system requirements or prerequisite actions. Use the following sections for this purpose:
   - UNIX: Brightmail Scanner
     - "Confirm Hardware Requirements," on page 15
     - "Confirm Software and Location Requirements," on page 16
     - "Create Required Accounts and Directories," on page 18
   - Windows: Brightmail Scanner
     - "Hardware Requirements," on page 43
     - "Software Environment," on page 43
   - UNIX and Windows: Brightmail Control Center
     - "Hardware Requirements," on page 57
     - "Software Environment Requirements," on page 58
     - "Operating System Compatibility," on page 58
2. Install at least one Brightmail Scanner as described in "Installing Brightmail Scanner for Sendmail," on page 19 or "Installing Brightmail Scanner for Windows," on page 46.

   NOTE: *If you are upgrading from a previous release you should upgrade ALL Brightmail Scanners prior to upgrading the Brightmail Control Center. See* "Upgrading Software," on page 21 *for UNIX Brightmail Scanners, or* "Upgrading Software," on page 44 *for Windows Brightmail Scanners.*
3. Install Brightmail Control Center as described in "Installing Brightmail Control Center on UNIX," on page 60 or "Installing Brightmail Control Center on Windows," on page 67.

4 Add a Brightmail Scanner using the Brightmail Control Center as described in "Adding a Brightmail Scanner," on page 77.

5 Make sure the Brightmail Scanner can be turned on by the Brightmail Control Center as described in "Starting a Brightmail Scanner from the Brightmail Control Center," on page 78.

6 Test that filtering is working as described in "Testing Symantec Brightmail AntiSpam Filtering," on page 78.

Installing Brightmail Scanner for Sendmail

This section describes how to prepare for and install Brightmail Scanner for Sendmail. Brightmail Scanner contains the Brightmail Agent and also contains either a Brightmail Server, a Brightmail Client or both a Brightmail Server and a Brightmail Client.

The following sections describe how to install Brightmail Scanner:

- Preparing to Install Brightmail Scanner
- Installing Brightmail Scanner for Sendmail
- What to Do Next
- Uninstalling Brightmail Scanner for Sendmail

NOTE: *If you are upgrading from Version 6.0 or Version 6.0.1, refer to* "Upgrading Software," on page 21.

Preparing to Install Brightmail Scanner

This section contains details of what needs to be done before installing Brightmail Scanner. Use the following sections for information on how best to prepare for the installation of Brightmail Scanner.

- Confirm Hardware Requirements
- Confirm Software and Location Requirements
- Enable Sendmail External Filtering
- Create Required Accounts and Directories

Confirm Hardware Requirements

The number of Brightmail Scanner computers you deploy depends on your message volume. The minimum suggested configuration requirements for each Brightmail Scanner computer include:

- Solaris
  - UltraSPARC processor
  - 512 MB RAM minimum (1 GB or more recommended)
  - 250 MB disk space minimum (1 GB or more recommended)

- Linux
  - Intel Pentium or compatible III or IV processor
  - 512 MB RAM minimum (1 GB or more recommended)
  - 250 MB disk space minimum (1 GB or more recommended)

For more information on hardware requirements, see the *Symantec Brightmail AntiSpam Deployment Planning Guide*.

Confirm Software and Location Requirements

This version of Symantec Brightmail AntiSpam is supported for Sendmail on the following operating systems and contains these additional software requirements:

- **Solaris**
  - Solaris 8 or 9

  For Solaris 8, patch 112438 is required.

  Because the `tar` file names exceed the 40 character file name limit of native Solaris `tar`, GNU tar is required to install Symantec Brightmail AntiSpam. GNU `tar` for Solaris is available from `http://www.sunfreeware.com` and other web sites.
- **Linux**
  - Red Hat Enterprise Linux AS 3.0
  - Red Hat Enterprise Linux ES 3.0

  For Linux installations, the Installer requires the `compat-libstdc++` library. The `compat-libstdc++` library is available on your Red Hat distribution CD.
- **A fully qualified domain name is required for each computer running Brightmail Scanner.**
- **Sendmail 8.12.11 or later or Sendmail Switch 3.1**
- **Sendmail Filtering**

  You must enable the Sendmail Milter API. For more information, see "Enable Sendmail External Filtering," on page 17.

  You can use the Sendmail restricted shell (`smrsh`) to run executables. For information, refer to the Sendmail documentation and the Sendmail `README` file.
- **Root access** using `su` or `sudo`
- **82 MB of free disk space** for the installed files
- **172 MB of free `/tmp` disk space** for use during installation

  You can set the environment variable `IATEMPDIR` to an alternate temporary storage directory if your `/tmp` directory does not have enough space.
- **Outbound Access by Brightmail Server to TCP port 443**

  Open port 443 on your firewall for HTTPS communication. For registration and ongoing operations, Symantec Brightmail AntiSpam communicates with the BLOC

over a secure connection. Consequently, TCP port 443 must be configured to allow outbound connections.

NOTE: *Symantec Brightmail AntiSpam's ability to identify spam accurately depends on having access to messages in their original form. Software and hardware which modify message headers and/or the content or structure of message bodies may undermine Symantec Brightmail AntiSpam's effectiveness.*

Enable Sendmail External Filtering

Your Sendmail installation must have support enabled for the Mail Filter API (Milter). Milter is necessary to support external mail filters, such as the Brightmail Filter.

To verify if you have Milter support enabled, type the following command:

```
/usr/lib/sendmail -bt -d0 < /dev/null
```

The system displays text similar to the following:

```
Version 8.12.11
 Compiled with: DNSMAP LOG MAP_REGEX MATCHGECOS MILTER MIME7TO8 MIME8TO7
                NAMED_BIND NDBM NETINET NETINET6 NETUNIX NIS NISPLUS
                PIPELINING SCANF XDEBUG
```

If you see a reference to `MILTER`, then your Sendmail installation has the required Milter support and you can skip this section.

Otherwise, follow the steps below to add the necessary lines to the build configuration file in the Sendmail directory and build a new version of Sendmail. If you have problems building and configuring Sendmail, refer to the following configuration document: `http://www.milter.org/milter_api/installation.html`. If you do not have the Sendmail source, you can find it on the Sendmail Web site: `http://www.sendmail.org`.

NOTE: *For more information on setting up Sendmail see* "Configuring Sendmail for the Brightmail Filter," on page 33.

To compile Sendmail 8.12 to use external mail filters:

1. Log in as `root`.
2. Change to your base `sendmail` directory and open the build configuration file (located at `devtools/Site/site.config.m4`).

   You can create this file if it doesn't exist.
3. Add the following line:

   ```
   APPENDDEF(`conf_sendmail_ENVDEF', `-DMILTER')
   ```
4. Save your changes to the build configuration file.

5 In the sendmail directory, type the following to build Sendmail 8.12 with the new settings:

```
# sh Build -c
```

6 To verify external filter support, type the following:

```
# /usr/lib/sendmail -bt -d0 < /dev/null
```

The system displays text similar to the following. Be sure to check the text for references to MILTER.

```
Version 8.12.11
 Compiled with: DNSMAP LOG MAP_REGEX MATCHGECOS MILTER MIME7TO8 MIME8TO7
                NAMED_BIND NDBM NETINET NETINET6 NETUNIX NIS NISPLUS
                PIPELINING SCANF XDEBUG
```

Create Required Accounts and Directories

Brightmail Scanner runs as user mailwall in the bmi group. Do not change these settings.

1 Before you install Brightmail Scanner, create the bmi group and the mailwall user in the bmi group. The following steps describe one way to do this. You can use different tools to perform this task.

For Solaris users:

```
$ su
Password: your_root_password
# groupadd bmi
# useradd -c "dummy user for Brightmail" -d /opt/symantec/sbas/Scanner -m -g \
   bmi mailwall
```

For Linux users:

```
$ su
Password: your_root_password
# groupadd -r bmi
# useradd -c "dummy user for Brightmail" -d /opt/symantec/sbas/Scanner -m -r \
   -g bmi mailwall
```

NOTE: *The -r flag (Red Hat Enterprise Linux only) places the specified user or group into a specific range of account IDs used for system accounts.*

2 Next, create a mail alias for the mailwall account so that all mail sent to mailwall is read by an administrator.

Installing Brightmail Scanner for Sendmail

Table 2 describes the ways to invoke the Installer when installing Brightmail Scanner.

Table 2. Installer Invocation Methods

Method	Command	Description
Command Line	`install`	The Installer prompts are presented in the terminal window in which you started the Installer.
Graphical User Interface (GUI)	`install -i awt`	The Installer prompts are presented using X Windows. To use this GUI installation, X Windows must be installed and configured correctly on your system.

The prompts for the command line and GUI installation are the same. Only the command line installation is presented in this guide. During installation, you can return to the previous question (go back) or quit at any time.

The Installer creates the following default mail-handling characteristics:

- Symantec Brightmail AntiSpam filters email addressed to all domains
- All spam messages will have their Subject line modified, such that it begins with `[Spam]`
- All viruses detected in messages will be cleaned and the cleaned messages will be delivered to the inbox

NOTE: *These settings, along with many others, can be adjusted using the Brightmail Control Center. For more information about doing so please refer to the Symantec Brightmail AntiSpam Administration Guide.*

Find and Run the Install Script

An install script has been prepared for Linux and Solaris installations of Brightmail Scanner. The install script ensures access to the correct libraries for Linux installations, and provides the appropriate Java runtime environment for the Installer.

To locate the Install Script:

1. Make sure you have created the `mailwall` user and `bmi` group as described in "Create Required Accounts and Directories," on page 18.

   The Installer won't run if you haven't done this.

2. Do one of the following to navigate to the install script based on whether you are installing from a CD-ROM or a downloaded file:

   If you are installing from a CD-ROM:

   a. Insert the CD containing Symantec Brightmail AntiSpam software into the CD-ROM drive.

   The CD will mount automatically to `/cdrom/bas_60x` on Solaris systems.

b. If you are using Linux, mount the CD-ROM.

```
$ mount /dev/cdrom
```

This command can fail if you've modified `/etc/fstab` on your system.

c. If you are using Linux, type:

```
$ cd /mnt/cdrom
```

d. Change to the appropriate directory for your CD-ROM.

```
$ cd operating_system
```

You will see the following top-level directories and files:

Table 3. Linux/Solaris Directories and Files for Brightmail Scanner Installation

File or Directory	Contents
EULA	File containing the End User License Agreement
`install`	Install script to prepare system and run the Installer
`scanner_install_`*`platform`*`.bin`	Installer binary for Solaris or Linux, invoked by the `install` script
`documentation.html`	List of available documentation

e. Locate the two files, `install` and EULA.

If you are installing from a downloaded tar file:

a. Change to the directory that contains the Symantec Brightmail AntiSpam software.

b. Untar the distribution file.

```
For Solaris:
$ tar -zxvf BAS_60x_sparc_solaris.tgz
```

```
For Linux:
$ tar -zxvf BAS_60x_x86_linux.tgz
```

c. Locate the two files, `install` and EULA.

For a directory listing see Table 3.

3 Open and read the file named EULA.

You should read this End User License Agreement before performing the installation.

4 If you are using a previous version, read the next section. If not, continue with "Installing with the Command-Line Installer," on page 23.

Upgrading Software

You must upgrade all of your Brightmail Scanners before you upgrade your Brightmail Control Center. You can upgrade from either Version 6.0 or Version 6.0.1. Upgrading or migrating data from Version 5.5 or earlier versions is not supported. Use of the **Settings** > **Migration** page in the Brightmail Control Center is not supported.

Follow the instructions in "To upgrade from Version 6.0 or Version 6.0.1 to Version 6.0.2:" below.

However, if you want to do either of the following, follow the instructions in "Uninstalling Version 6.0 or 6.0.1 and installing Version 6.0.2," on page 22:

- Install the Version 6.0.2 Brightmail Scanner into a different folder than the folder where your current Version 6.0.x Brightmail Scanner resides.
- Change the selection of components on this Brightmail Scanner (Brightmail Server, Brightmail Client or both).

To upgrade from Version 6.0 or Version 6.0.1 to Version 6.0.2:

1. From the Brightmail Scanner computer, stop all Scanner processes using the following command, as root:

```
# /etc/init.d/mailwall stop
```

2. Follow the instructions in, "Installing with the Command-Line Installer," on page 23. As you perform the installation, note the following:
   a. When asked to specify your Brightmail Control Center, your answer can differ from the current (Version 6.0.x) configuration of this Brightmail Scanner.
   b. When asked to choose your installation type, your choice (Complete, Brightmail Server or Brightmail Client) must match the current (Version 6.0.x) configuration of this Brightmail Scanner.
   c. Although you may be asked to register again, you do not need to register again.
3. From the Brightmail Scanner computer, start all Scanner processes using the following command, as root:

```
# /etc/init.d/mailwall start
```

4. Before upgrading your Brightmail Control Center, upgrade each Brightmail Scanner in your system.
5. Follow the instructions in "Installing Brightmail Control Center," on page 57 to upgrade your Brightmail Control Center.
6. After upgrading all Brightmail Scanners and the Brightmail Control Center, you can make any configuration changes needed from the Brightmail Control Center.

Uninstalling Version 6.0 or 6.0.1 and installing Version 6.0.2

If you uninstall and reinstall, you may need to register. First, decide which of the following four scenarios applies to you, then follow the appropriate instructions.

- The Brightmail Scanner you are installing does not include a Brightmail Server. You therefore do not need to register. See "To uninstall Version 6.0 or 6.0.1 and install Version 6.0.2:", and ignore step 4.
- You are currently on a free trial, and you plan to install in a different directory for production use. See "To uninstall Version 6.0 or 6.0.1 and install Version 6.0.2:".
- Your license is about to expire. See "To uninstall Version 6.0 or 6.0.1 and install Version 6.0.2:".
- Your license is not due to expire soon. See "To uninstall Version 6.0 or 6.0.1 and install Version 6.0.2 using an existing license key:".

To uninstall Version 6.0 or 6.0.1 and install Version 6.0.2:

1. From the Version 6.0.x Brightmail Control Center, remove the Version 6.0.x Brightmail Scanner.
2. From the Brightmail Scanner computer, stop the Scanner, using the following command, as root:

```
# /etc/init.d/mailwall stop
```

3. Uninstall the Version 6.0.x Brightmail Scanner.
4. Install the Version 6.0.2 Brightmail Scanner.
5. If your Version 6.0.2 Brightmail Scanner includes a Brightmail Server, you must register the Brightmail Scanner.

   NOTE: *Because Symantec is now using (as of Version 6.0.1) a different licensing technology for this product, to register you must contact your Symantec sales person or go to the following URL:* `http://www.symantecstore.com/renew`.

6. Before installing your Brightmail Control Center, upgrade each Brightmail Scanner in your system.
7. Install the Version 6.0.2 Brightmail Control Center.
8. From the Version 6.0.2 Brightmail Control Center, add the Brightmail Scanners.

To uninstall Version 6.0 or 6.0.1 and install Version 6.0.2 using an existing license key:

1. Make a backup copy of the `cert.pem` file, which you can find in the `etc` directory under your installation directory.
2. Uninstall Version 6.0.x.
3. In your new installation directory, create a new directory named: `etc`

4 Copy the backup `cert.pem` file into the `etc` directory you created.

5 Install Version 6.0.2 into your new installation directory.

6 Before installing your Brightmail Control Center, upgrade each Brightmail Scanner in your system.

7 Install the Version 6.0.2 Brightmail Control Center.

8 From the Version 6.0.2 Brightmail Control Center, add the Brightmail Scanners.

When your license key expires you will need to register using a license (`.slf`) file. To purchase one, contact your Symantec sales person or go to the following URL: `http://www.symantecstore.com/renew`. Then follow the instructions in "Registering to Receive New AntiSpam Filters," on page 30.

Installing with the Command-Line Installer

NOTE: *When running on Red Hat Enterprise Linux, the Installer requires the presence of the* `compat-libstdc++` *library. If this library is not on your machine, the Installer will stop and ask you to install the library before you install Brightmail Scanner. The* `compat-libstdc++` *library is available on your Red Hat distribution CD.*

1 As `root` user, run the Installer:

```
$ su root -c './install'
Password: your_root_password
```

2 If you have the binary for the Brightmail Control Center in the same directory as Brightmail Scanner binary, you will be prompted to select an installation as shown in the following example. Otherwise, installation begins immediately.

```
Installers for both Brightmail Control Center and
   Brightmail Scanner software are present and available to
   be installed.
Please select one of the following:
        1 -     Brightmail Scanner
        2 -     Brightmail Control Center
        q -     Quit or Exit
Which software would you like to install? 1
```

3 Choose `1` from the menu if you see the above screen and press `Enter` to install Brightmail Scanner.

The install script runs, prepares your system as required, and then runs the Installer. The Installer displays introductory text.

```
Introduction
------------

This installer will guide you through the installation of Brightmail
   Scanner, part of Symantec Brightmail AntiSpam.

Respond to each prompt to proceed to the next step in the installation.
If you want to change something on a previous step, type 'back'.
You may cancel this installation at any time by typing 'quit'.
PRESS <ENTER> TO CONTINUE:
```

4 At the first prompt, read the License Agreement if you have not already done so and indicate whether or not you accept it as provided. To accept the license agreement, type `1`.

```
License Agreement
-----------------

Do you agree to the terms and conditions covered in the license agreement:
/your_installer_path/EULA ?

    1- Yes
  ->2- No

ENTER THE NUMBER FOR YOUR CHOICE, OR PRESS <ENTER> TO ACCEPT THE DEFAULT:
   : 1
```

5 At the next prompt, choose the installation directory—the path to Brightmail Scanner files. To accept the recommended path, press Enter.

```
Choose Install Folder
---------------------

Where would you like to install Brightmail Scanner?

  Default Install Folder: /opt/symantec/sbas/Scanner

ENTER AN ABSOLUTE PATH, OR PRESS <ENTER> TO ACCEPT THE DEFAULT
      :
```

NOTE: *If you are upgrading from Version 6.0 or Version 6.0.1, you will not be asked for the installation directory location. The existing installation will be upgraded to 6.0.2.*

NOTE: *While acceptable, setting the location of the installation directory to a remotely mounted partition is not recommended. If you do so, the Installer issues a warning and prompts you to set it to a local partition.*

NOTE: *If you choose to enter information at this prompt, be very careful not to insert any spaces as you type. Spaces are not stripped from input that you enter, and they can cause the installation to fail.*

If you have already installed Brightmail software, but choose a different directory, the Installer will place the software in the newly specified directory, without modifying the original directory.

```
INSTALL FOLDER IS: /opt/symantec/sbas/Scanner
   IS THIS CORRECT? (Y/N): y
```

6 At the next prompt, confirm the location of the log folder. This is the directory where notifications and errors are stored by default.

```
Choose Log Folder
-----------------

Choose a folder where logs will be saved.

Log Folder (DEFAULT: /var/log/brightmail):
```

NOTE: *If you choose to enter information at this prompt, be very careful not to insert any spaces as you type. Spaces are not stripped from input that you enter, and they can cause the installation to fail.*

7 At the next prompt, provide the location for the Brightmail Control Center.

```
Specify Brightmail Control Center
---------------------------------

For security purposes, you must specify the computer which is running
or will be running the Brightmail Control Center. Only servers
   defined here will be allowed to configure this Scanner.

  ->1- This computer
    2- Computer at IP Address
    3- Any computer (security risk; check Installation Guide for
       details)
ENTER THE NUMBER FOR YOUR CHOICE, OR PRESS <ENTER> TO ACCEPT THE
   DEFAULT:
    : 1
```

Choose `This Computer` if you are planning on a single-machine installation of a Brightmail Scanner and a Brightmail Control Center. Choose `Computer at IP Address` to allow the attachment of a different but specific computer as the Control Center for this Brightmail Scanner. Choose `Any computer` to allow the attachment of any computer as the Control Center for this Brightmail Scanner.

NOTE: *Depending on your network security architecture, choosing* `Any computer` *could pose a security risk, because it allows this Brightmail Scanner to be controlled from any computer that has HTTPS access to this computer.*

8 At the next prompt, specify the installation type:

```
Choose Installation Type
------------------------

Please choose the Install Set to be installed by this Installer.

  ->1- Complete Installation
    2- Brightmail Server only
    3- Brightmail Client only

ENTER THE NUMBER FOR THE INSTALL SET, OR PRESS <ENTER> TO ACCEPT THE
   DEFAULT
    : 1
```

Complete Installation – Installs all components of a Brightmail Scanner, including support for the Sendmail integration and the Brightmail Server. Sendmail needs to be on the same machine as the Brightmail Scanner installation.

Brightmail Server only – Installs all server components of a Brightmail Scanner. No Sendmail integration is installed. Sendmail does not need to be on the same machine as the Brightmail Scanner installation.

Brightmail Client only – Installs only the Brightmail Client integration for Sendmail with no Brightmail Server components. Sendmail needs to be on the same machine as the Brightmail Scanner installation. It is not necessary to register a Brightmail Scanner when performing a client-only installation.

NOTE: *If you are upgrading from Version 6.0 or 6.0.1 to Version 6.0.2, choose the same components currently configured on your Version 6.0.x Brightmail Scanner.*

At the next prompt, a summary of the choices you've made is displayed.

```
Pre-Installation Summary
------------------------

Please review the following before continuing:

Product Name:
    Brightmail Scanner

Install Folder:
    /opt/symantec/sbas/Scanner

Install Set
    Complete Installation

Log Folder:
    /var/log/brightmail


PRESS <ENTER> TO CONTINUE:
```

9 When performing a client-only installation, you will see this screen after accepting the installation summary:

```
Server Address
--------------

You have chosen a client only install. Please enter the IP address of
the machine on which a Brightmail Server is or will be available:

Server address (DEFAULT: 127.0.0.1): 10.10.208.27
```

Supply the IP address for the Brightmail Server to which you wish to connect this client. It is not necessary for the Brightmail Server to be already installed.

10 Press `Enter` to install the product based on these settings.

Next, `Installing...` appears on the screen, and a progress bar is displayed.

```
Installing...
-------------


[================|================|================|==============]
[----------------|--------
```

You are now ready to register Brightmail Scanner. This is necessary if your installation included the Brightmail Server. It is important to have available the path to your Symantec license file and any proxy information required if your company is using a firewall.

However, if you are upgrading Symantec Brightmail AntiSpam from Version 6.0 or 6.0.1 to Version 6.0.2, continue using your previous license by answering `No` on the `Registration` screen. When your license expires, see "Registering to Receive New AntiSpam Filters," on page 30 for instructions on obtaining and implementing a new license.

11 When you see the following screen, press `ENTER` to begin registration. If you choose not to register Brightmail Scanner, or if registration fails, see "Registering to Receive New AntiSpam Filters," on page 30 for additional information.

```
Registration
------------

Please register your Brightmail installation now.

If you choose not to, you will not be able to receive
Symantec Brightmail AntiSpam filters until registration
is complete.

Do you want to register now?
->1- Yes
  2- No

ENTER THE NUMBER FOR YOUR CHOICE, OR PRESS <ENTER> TO ACCEPT THE
  DEFAULT:
   :
```

In the registration process, you are first asked to provide the path to your license file, which Symantec uses to identify you as a valid customer and through which filter delivery is tracked.

For new customers, your license file is an `.slf` file you acquired via Symantec's Enterprise Licensing System (ELS) when you purchased Symantec Brightmail AntiSpam. If you choose not to register, you can do so later.

```
Input License File Path
-----------------------
Please Enter your License File Path.

License File Path: (DEFAULT: none):
```

12 Type the path to your license file carefully and press Enter. For example:

```
/home/user/license.slf
```

Then, you are asked to provide any proxy information that is required to allow your registration information to be transmitted to the BLOC.

```
Proxy Use
---------

Will you use an HTTPS proxy?

    1- Yes
  ->2- No

ENTER THE NUMBER FOR YOUR CHOICE, OR PRESS <ENTER> TO ACCEPT THE
   DEFAULT:
    :
```

13 Type `1` if you are using a proxy server (you will then be asked for more proxy information), otherwise press Enter.

You have now completed the installation and registration process. A confirmation screen will be presented to give you complete status on your installation.

```
Install Complete

Brightmail Scanner has been successfully installed and a
default configuration file has been installed.

Before this Brightmail Scanner can filter email, you must install the
Brightmail Control Center and add this Brightmail Scanner.

Login to the Brightmail Control Center and configure this Brightmail
   Scanner.

PRESS <ENTER> TO EXIT THE INSTALLER:
```

In addition to the listed installation confirmation items, the Installer also:

- Sets the permissions for the installation directory to give access to user `mailwall`
- Creates the Runner configuration file, `runner.cfg`
- Adds a line for the AntiVirus Cleaner to the crontab of user `mailwall`
- Installs the Brightmail Scanner script, which lets you start, stop, or restart the Brightmail Scanner. This script is located in `/etc/init.d`.

Starting a Brightmail Scanner

The Brightmail Scanner cannot filter email messages until it is added to the Brightmail Control Center. Before adding the Brightmail Scanner to the Brightmail Control Center, you must start the Brightmail Scanner using the following command, as root, to allow the Brightmail Control Center to find and attach the Brightmail Scanner:

```
# /etc/init.d/mailwall start
```

After adding the Brightmail Scanner to the Brightmail Control Center, as described in "Adding a Brightmail Scanner," on page 77, you can use the Status page on the Brightmail Control Center to start and stop the Brightmail Scanner and its components.

Registering to Receive New AntiSpam Filters

During Brightmail Scanner installation, you are given the chance to register Brightmail Scanner when the installation includes the Brightmail Server. While unregistered, the Brightmail Scanner cannot receive new AntiSpam Filters. When you run the Brightmail Control Center and attempt to start an unregistered Brightmail Scanner, Brightmail Scanner remains disabled.

If your license key is expired, you will need to obtain an `.slf` file from your Symantec sales person or from `http://www.symantecstore.com/renew` and register after successful installation. After obtaining your license file, follow these steps to register:

To register after installation:

1. As `root` user, from the */opt/symantec/sbas/Scanner/***sbin** directory, run the registration script:

```
$ su root
# cd /opt/symantec/sbas/Scanner/sbin
# register.sh
```

2. The script asks for your license file:

```
# Please enter the path to a valid license file:
```

3. Enter the absolute path to the location of your `.slf` file.

What to Do Next

After successfully installing Brightmail Scanner, only a few additional steps remain to get Symantec Brightmail AntiSpam fully operational. Here is a recommended procedure to finish and test Symantec Brightmail AntiSpam setup for your installation.

1. Configure Sendmail to accommodate the Brightmail Filter as described in "Configuring Sendmail for the Brightmail Filter," on page 33.
2. If you have not done so already, manually start the Brightmail Scanner using the following command, as root:

```
# /etc/init.d/mailwall start
```

   The Brightmail Scanner cannot filter email messages until it is added to the Brightmail Control Center. Manually starting it this one time allows the Brightmail Control Center to find and attach this Brightmail Scanner.
3. Install the Brightmail Control Center as described in "Installing Brightmail Control Center," on page 57.
4. Add the Brightmail Scanner you installed and started as described in "Adding a Brightmail Scanner," on page 77.
5. Test filtering of spam as described in "Testing Symantec Brightmail AntiSpam Filtering," on page 78.

Uninstalling Brightmail Scanner for Sendmail

To uninstall this version of Brightmail Scanner for Sendmail, use the provided uninstall script. This script will remove files and directories that were initially installed with the install script. However, files that were modified since installation won't be removed, such as antispam filters.

Uninstalling with the Command-Line Installer

To remove Brightmail Scanner software:

1. Run the Uninstaller as the `root` user:

```
$ su root -c '/opt/symantec/sbas/Scanner/UninstallerData/Uninstall'
Password: your_root_password
```

The Uninstaller prints out status messages similar to the following as it removes the Brightmail software:

```
Preparing CONSOLE Mode Installation...

===============================================================================
Symantec Brightmail AntiSpam (created with InstallAnywhere by Zero G)
-------------------------------------------------------------------------------

===============================================================================
About to uninstall...
---------------------

This will remove features installed by InstallAnywhere.  It will not remove
files and folders created after the installation.

PRESS <ENTER> TO CONTINUE:

===============================================================================
Uninstalling...
---------------

...*
*
*************************
*************************
*************************
*************************


===============================================================================
Uninstall Complete
------------------

All items were successfully uninstalled.
```

The Brightmail Scanner is now uninstalled.

Configuring Sendmail for the Brightmail Filter

The Brightmail Client communicates with the Sendmail MTA using the standard Sendmail Mail Filter API. To implement this integration, the Brightmail Client uses the Brightmail Filter (`bmifilter`), an intermediary program, which connects to Sendmail over a socket connection. The Brightmail Filter program also controls client-side actions such as removing mail and tagging spam. This section tells you how to enable filtering and the Brightmail Filter in Sendmail. This section includes the following topics:

- Understanding the Filter Address and Optional Settings
- Configuring Sendmail Switch to Work with Brightmail Scanner
- Configuring Sendmail for Brightmail Scanner with sendmail.cf
- Configuring Sendmail for Brightmail Scanner with M4

Based on the version of Sendmail you are using, do the following:

- If you are using Sendmail Switch, use the Sendmail Administration Console to define the filter. See "Configuring Sendmail Switch to Work with Brightmail Scanner," on page 35.
- If you are using Sendmail 8.12.11 or later, either manually edit the `sendmail.cf` file, or if using an m4 file, edit that file. See "Configuring Sendmail for Brightmail Scanner with sendmail.cf," on page 40 or "Configuring Sendmail for Brightmail Scanner with M4," on page 41.

NOTE: *During installation, the Brightmail Filter is configured to use port 41001, with a default setting of* `inet:41001`*. This Brightmail Filter port number must correspond to the port number for the* `Xbmifilter` *setting in Sendmail specified in this section.*

Understanding the Filter Address and Optional Settings

In Sendmail 8.12.11, and later, the `X` setting has the following format:

```
Xbmifilter,S=inet:port_number@machine.your_domain.com
```

Where:

port_number is the valid networking port number that you configured for the bmifilter program.

machine is the IP address or DNS name of the machine that is running bmifilter.

You can also specify the behavior when Sendmail cannot connect to the Brightmail Filter. You can configure Sendmail to:

- Temporarily reject the message with an SMTP 4xx instruction. To specify this behavior, add the F=T flag to the X setting.
- Permanently reject the message with an SMTP 5xx instruction. To specify this behavior, add the F=R flag to the X setting.
- Accept the message and send it through (as if the Brightmail Filter was not present). You specify this behavior by omitting the F= option.
- Specify a timeout period. To do this, add the T=C flag to the X setting.

The following example omits the F= flags so that Sendmail accepts messages if it cannot connect to the Brightmail Filter:

```
Xbmifilter, S=inet:41001@machine.your_domain.com
```

Where:

machine is the host to which Sendmail will connect. If you do not specify a machine name, Sendmail will try to connect on the same machine.

NOTE: *In Sendmail Switch, you specify the filter name, filter address and optional settings differently.You type* bmifilter *in the Filter Name field, and the filter address and optional settings in the Equates field of the INPUT_MAIL_FILTERS() option. See* "Configuring Sendmail Switch to Work with Brightmail Scanner," on page 35 *for more information.*

The following example shows the use of the T= flag to specify a timeout period:

This example may not be optimal for your environment.

```
Xbmifilter, S=inet:41001@machine.your_domain.com, F=T, T=C:10m;S:1m;R:1m;E:10m
```

Where:

C is the connect timeout, S is the send timeout, R is the receive timeout, E is the total timeout, and m represents minutes.

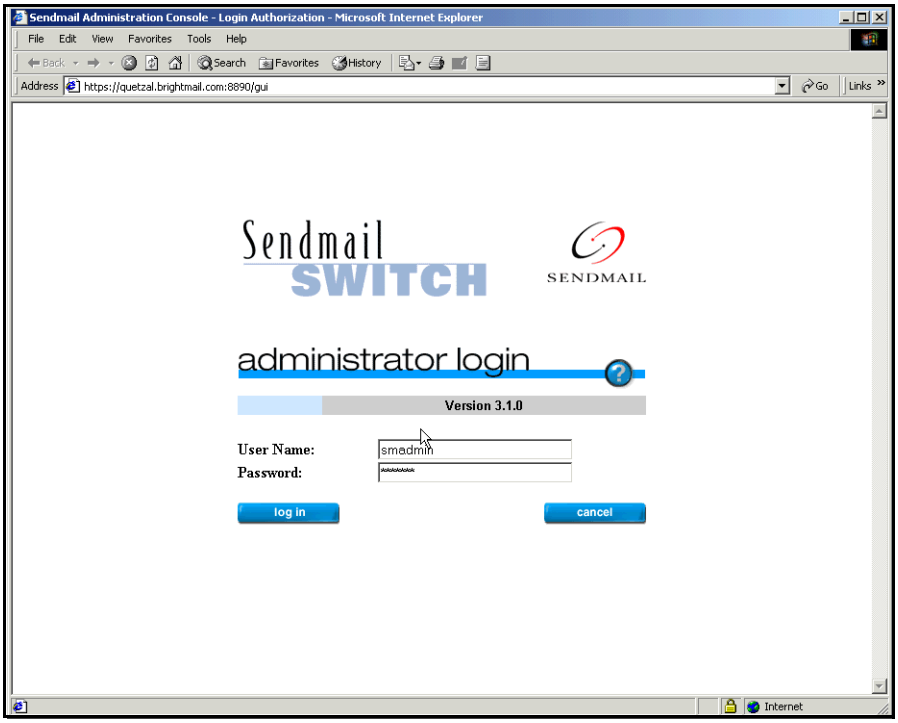
To specify both F= and T= flags, separate them with a comma followed by a space as shown. For more information on the syntax for this setting, see: http://www.milter.org/milter_api/installation.html.

Configuring Sendmail Switch to Work with Brightmail Scanner

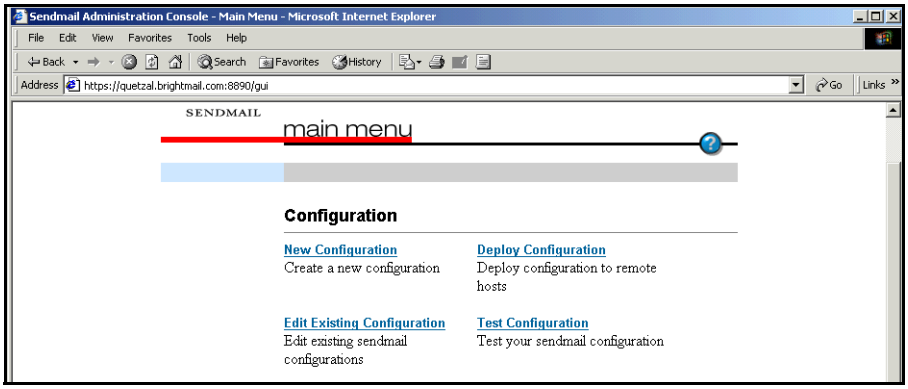
NOTE: *Before completing this procedure, make sure you have followed the instructions in* *"Enable Sendmail External Filtering," on page 17*.

To enable Sendmail Switch to work with a Brightmail Scanner:

1 Using the appropriate URL for your environment, open the Sendmail Administrator Console in a Web browser.

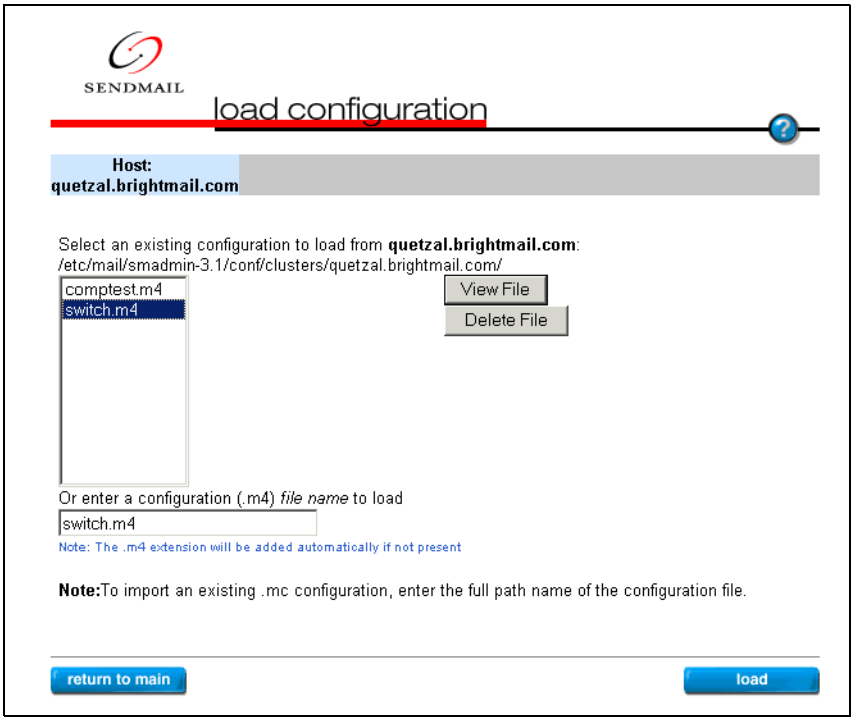


2 Log in to the Sendmail Administrator Console.

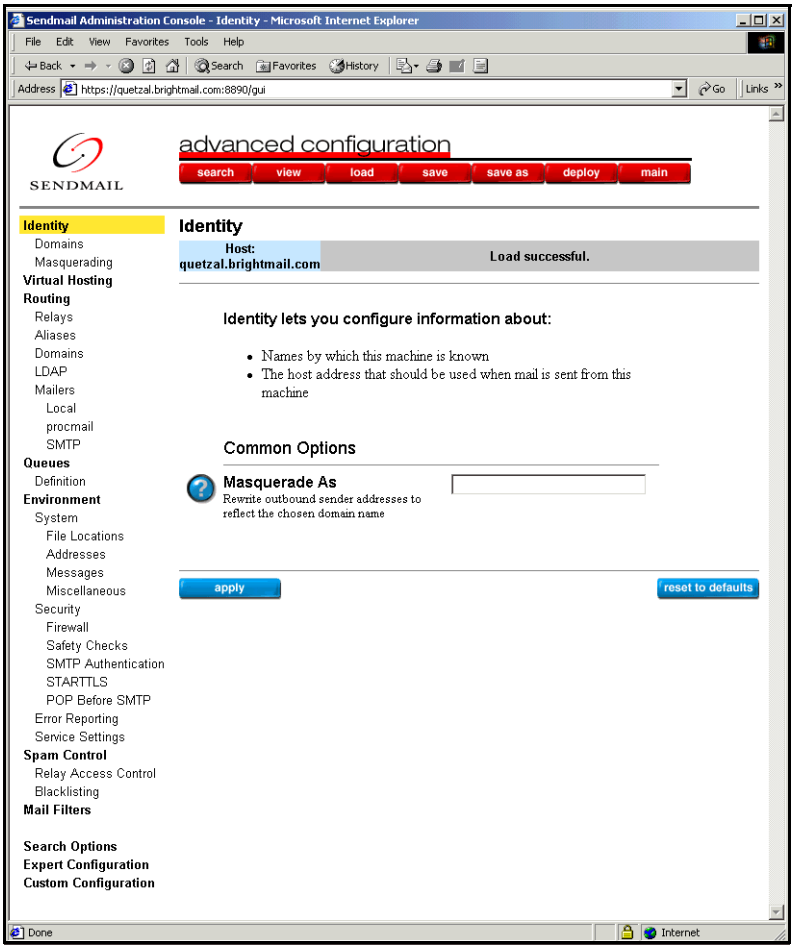


3 Click **Edit Existing Configuration**.

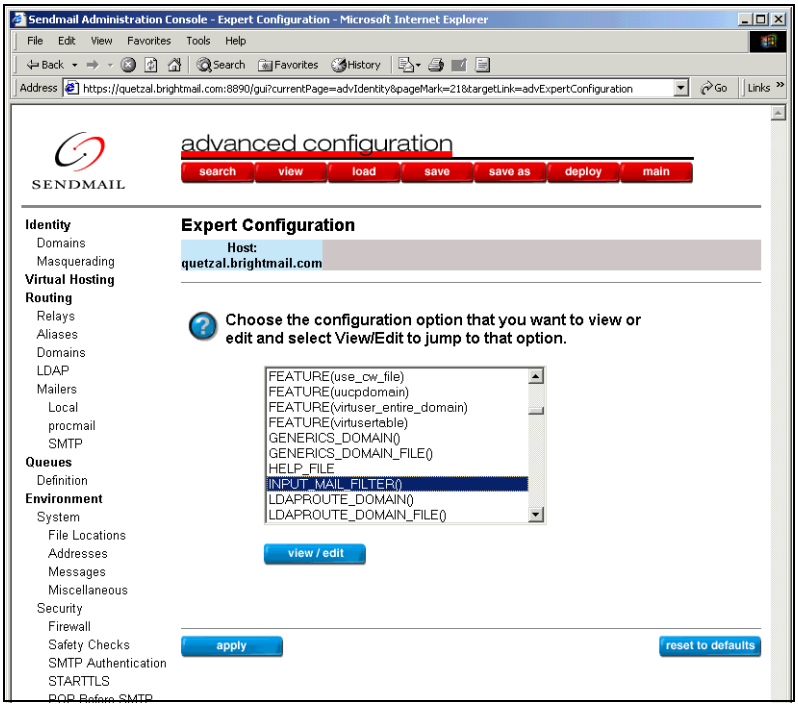
4 If necessary, select the host or cluster to configure, and then click **select**.



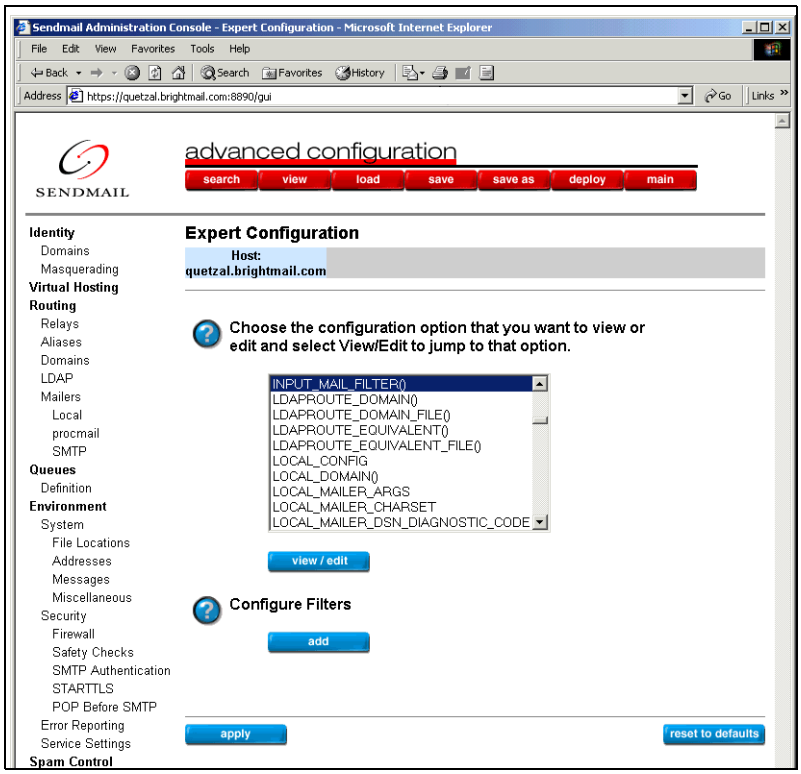
5 Highlight an existing configuration or type a configuration in the text field, and then click **load**.



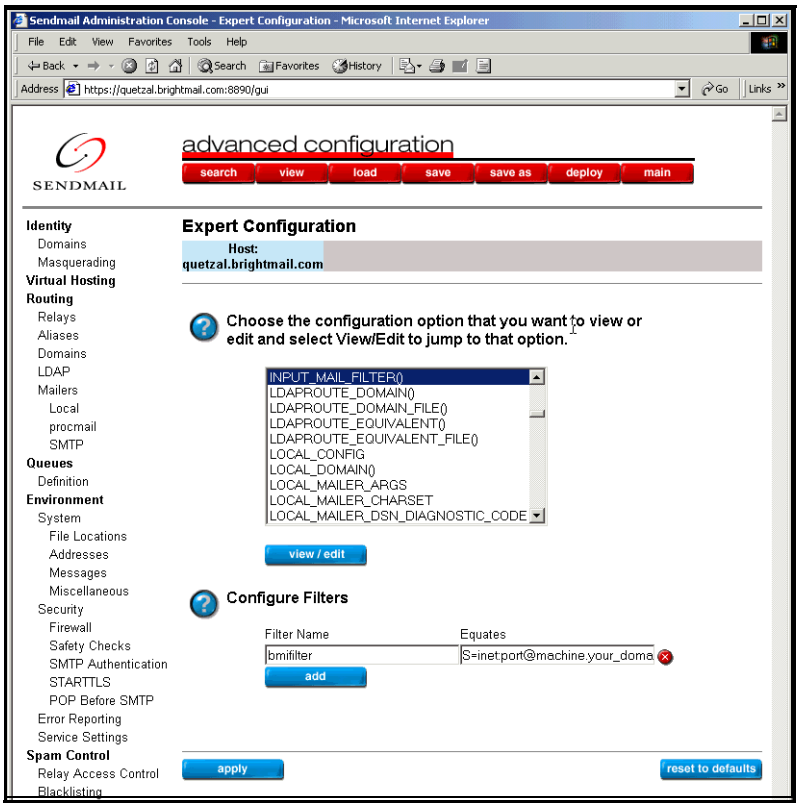
6 In the menu on the left side, click **Expert Configuration**.



7 In the scrolling list, select **INPUT_MAIL_ FILTERS()**, and then click **view/edit**.



8 Click **add**.



9 In the **Filter Name** field, type `bmifilter`.

10 In the **Equates** field, specify the filter address and any optional settings. The following example is appropriate in most cases:

```
S=inet:port@machine.xyz.com, T=C:10m;S:1m;R:1m;E:10m
```

See "Understanding the Filter Address and Optional Settings," on page 33 for information about the optional `F=` failure setting and the `T=` timeout setting.

NOTE: *The filter name and the filter executable name must be the same to monitor it from the Service Control page.*

11 Click **apply** to apply the filter.

12 Save your changes and deploy the configuration file.

Configuring Sendmail for Brightmail Scanner with sendmail.cf

There are two ways to configure Sendmail to work with Symantec Brightmail AntiSpam. You can either edit the `sendmail.cf` file, or you can use `m4` to generate a new `sendmail.cf` file. This section covers what you need to know to use `sendmail.cf` to configure Sendmail. To use `m4`, refer to "Configuring Sendmail for Brightmail Scanner with M4," on page 41.

NOTE: *Before completing this procedure, make sure you have followed the instructions in* "Enable Sendmail External Filtering," on page 17.

1. Log in as `root`.
2. Open the Sendmail configuration file, `sendmail.cf`, for editing. The `sendmail.cf` file is usually located in `/var/mail/sendmail.cf` or `/etc/mail/sendmail.cf`.
3. In the `OPTIONS` section, add the Brightmail Filter as follows:

```
OPTIONS
O InputMailFilters=bmifilter
```

4. In the `MAIL FILTER DEFINITIONS` section, enter the following line to complete the socket for the Brightmail Filter configuration:

```
Xbmifilter, S=inet:port@machine.your_domain.com
```

   Refer to "Understanding the Filter Address and Optional Settings," on page 33 for information on address values.

5. Save the file.
6. Stop Sendmail:

```
# /etc/init.d/sendmail stop
```

7. Verify that Sendmail is no longer running:

```
# ps -ef | grep sendmail
```

   If any processes are shown other than `grep`, send a `SIGTERM` to each process to terminate it:

```
# kill process_id
```

8. Restart Sendmail:

```
# /etc/init.d/sendmail start
```

9 Verify that Sendmail has restarted:

```
# ps -ef | grep sendmail
```

Configuring Sendmail for Brightmail Scanner with M4

There are two ways to configure Sendmail to work with Symantec Brightmail AntiSpam. You can either edit the sendmail.cf file, or you can use m4 to generate a new sendmail.cf file. This section covers what you need to know to use m4 to configure Sendmail. To use the sendmail.cf file, refer to "Configuring Sendmail for Brightmail Scanner with sendmail.cf," on page 40.

NOTE: *Before completing this procedure, make sure you have followed the instructions in* "Enable Sendmail External Filtering," on page 17.

If you are using an `m4` file, instead of editing `sendmail.cf`, you should edit your `m4` file to include the following command, and regenerate your `sendmail.cf` file as usual. This command must come after any `MAILER` line(s).

Also, see "Understanding the Filter Address and Optional Settings," on page 33 for timeout settings.

```
INPUT_MAIL_FILTER('bmifilter', 'S=inet:41001@machine.xyz.com, T=C:10m;S:5m;R:5m;E:10m')
```

Where:

`41001` is any valid networking port number that you configured for the `bmifilter` program.

`machine.xyz.com` is the IP address or DNS name of the machine that is running `bmifilter`.

Installing Brightmail Scanner for Windows

The following topics are covered in this section:

- Hardware Requirements
- Software Environment
- Upgrading Software
- Installing Brightmail Scanner for Windows
- Modifying, Repairing, and Removing Brightmail Scanner

Hardware Requirements

The number of Brightmail Scanner computers you should deploy depends on your message volume. The minimum suggested configuration requirements for each Brightmail Scanner computer include:

- Intel Pentium or compatible III or IV processor
- 512 MB RAM minimum (1 GB or more recommended)
- 250 MB disk space minimum (1 GB or more recommended)

For more information on hardware requirements, see the *Symantec Brightmail AntiSpam Deployment Planning Guide*.

Software Environment

The Brightmail Scanner requires the following:

- The Brightmail Scanner runs on Windows 2000 Server (SP2), Windows 2000 Advanced Server (SP2), Windows Server 2003, Standard Edition, or Windows Server 2003, Enterprise Edition.

  Caution

  The Brightmail Server is not an SMTP MTA and does not relay mail. Make sure your mail server is operational and relaying mail with the Windows SMTP Service, Exchange 2000, or Exchange 2003 before you install Symantec software. If you are using Exchange 5.5 as your MTA, see the Symantec Brightmail AntiSpam Deployment Planning Guide.

- The Brightmail Client requires Microsoft Internet Information Services (IIS) and the Windows SMTP service.
- Open port 443 on your firewall for HTTPS communication. For registration and ongoing operations, Symantec Brightmail AntiSpam communicates with the BLOC over a secure connection. Consequently, TCP port 443 must be configured to allow outbound connections.
- Administrator privileges on the local computer.

NOTE: *Symantec Brightmail AntiSpam's ability to identify spam accurately depends on having access to messages in their original form. Software and hardware which modify message headers and/or the content or structure of message bodies may undermine Symantec Brightmail AntiSpam's effectiveness.*

Upgrading Software

You must upgrade all of your Brightmail Scanners before you upgrade your Brightmail Control Center. You can upgrade from either Version 6.0.0 or Version 6.0.1. Upgrading or migrating data from Version 5.5 or earlier versions is not supported. Use of the **Settings** > **Migration** page in the Brightmail Control Center is not supported.

Follow the instructions in "To upgrade from Version 6.0.0 or 6.0.1 to Version 6.0.2:" below.

However, if you want to do either of the following, follow the instructions in "Uninstalling Version 6.0.0 or 6.0.1 and installing Version 6.0.2," on page 45:

- Install the Version 6.0.2 Brightmail Scanner into a different folder than the folder where your current Version 6.0.x Brightmail Scanner resides.
- Change the selection of components on this Brightmail Scanner (Brightmail Server, Brightmail Client or both).

To upgrade from Version 6.0.0 or 6.0.1 to Version 6.0.2:

1. Follow the instructions in, "Installing Brightmail Scanner for Windows," on page 46. As you perform the installation, note the following:
   a. When asked to specify your Brightmail Control Center, your answer can differ from the current (Version 6.0.x) configuration of this Brightmail Scanner.
   b. When asked to choose your installation type, your choice (Complete, Brightmail Server or Brightmail Client) must match the current (Version 6.0.x) configuration of this Brightmail Scanner.
   c. You do not need to re-register. However, if your license is expired, you will need to obtain an `.slf` file from your Symantec sales person or from `http://www.symantecstore.com/renew` and register after successful installation. See "To register after installation:," on page 46.
2. Before upgrading your Brightmail Control Center, upgrade each Brightmail Scanner in your system.

3 Follow the instructions in "Installing Brightmail Control Center," on page 57 to upgrade your Brightmail Control Center.

4 After upgrading all Brightmail Scanners and the Brightmail Control Center, you can make any configuration changes needed from the Brightmail Control Center.

Uninstalling Version 6.0.0 or 6.0.1 and installing Version 6.0.2

If you uninstall and reinstall, you may need to register. First, decide which of the following four scenarios applies to you, then follow the appropriate instructions.

- The Brightmail Scanner you are installing does not include a Brightmail Server. You therefore do not need to register. See "To uninstall Version 6.0.0 or 6.0.1 and install Version 6.0.2:", and ignore step 4.
- You are currently on a free trial, and you plan to install in a different directory for production use. See "To uninstall Version 6.0.0 or 6.0.1 and install Version 6.0.2:".
- Your license is about to expire. See "To uninstall Version 6.0.0 or 6.0.1 and install Version 6.0.2:".
- Your license is not due to expire soon. See "To uninstall Version 6.0.0 or 6.0.1 and install Version 6.0.2 using an existing license:," on page 45.

To uninstall Version 6.0.0 or 6.0.1 and install Version 6.0.2:

1 From the Version 6.0.x Brightmail Control Center, remove the Version 6.0.x Brightmail Scanner.

2 Uninstall the Version 6.0.x Brightmail Scanner.

3 Install the Version 6.0.2 Brightmail Scanner.

4 If your Version 6.0.2 Brightmail Scanner includes a Brightmail Server, you must register the Brightmail Scanner.

NOTE: *Because Symantec is now using a different licensing technology for this product, to register you must contact your Symantec sales person or go to the following URL:* `http://www.symantecstore.com/renew`.

5 Before installing your Brightmail Control Center, upgrade each Brightmail Scanner in your system.

6 Install the Version 6.0.2 Brightmail Control Center.

7 From the Version 6.0.2 Brightmail Control Center, add the Brightmail Scanners.

To uninstall Version 6.0.0 or 6.0.1 and install Version 6.0.2 using an existing license:

1 Make a backup copy of the `cert.pem` file, which you can find in the `etc` directory under your installation directory.

2 Uninstall Version 6.0.x.

3 In your new installation directory, create a new directory named: `etc`

4 Copy the backup `cert.pem` file into the `etc` directory you created.

5 Install Version 6.0.2 into your new installation directory.

6 Before installing your Brightmail Control Center, upgrade each Brightmail Scanner in your system.

7 Install the Version 6.0.2 Brightmail Control Center.

8 From the Version 6.0.2 Brightmail Control Center, add the Brightmail Scanners.

When your license key expires you will need to register using a license (`.slf`) file. To purchase one, contact your Symantec sales person or go to the following URL: `http://www.symantecstore.com/renew`

To register after installation:

1 Find and run the Registration Wizard. By default this file, `regwizard.exe`, is located in `C:\Program Files\Symantec\SBAS\Scanner\bin`.

2 Follow the instructions on page 52.

Installing Brightmail Scanner for Windows

To install Brightmail Scanner:

1 Close all open applications before installing Symantec software.

In particular, be sure to close the Services dialog box from the Administration Tools program group if it is open. If you don't, the installation may fail.

2 Do one of the following to navigate to the `Setup.exe` file:

If you are installing from a CD-ROM:

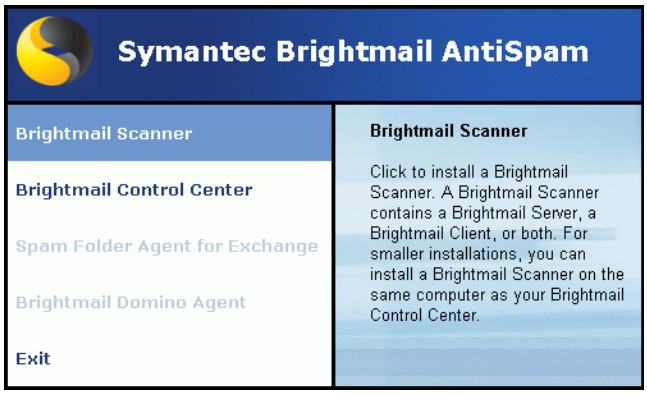
Insert the Symantec software distribution CD-ROM in your computer's CD-ROM drive.

If the Installer does not run automatically, open the **Windows** folder on the CD using Windows Explorer and double-click the **Setup.exe** icon.

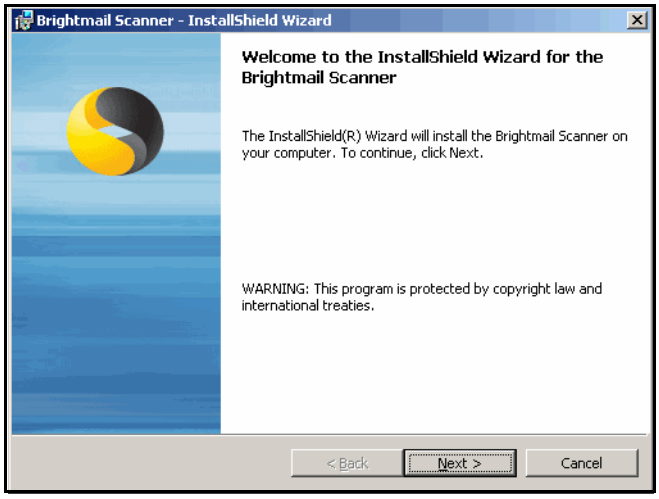
If you are installing from a downloaded zip file:

a. Unzip the zip file.

b. Double-click the **Setup.exe** icon.


Symantec Brightmail AntiSpam
Brightmail Scanner
Brightmail Control Center
Spam Folder Agent for Exchange
Brightmail Domino Agent
Exit
Brightmail Scanner
Click to install a Brightmail Scanner. A Brightmail Scanner contains a Brightmail Server, a Brightmail Client, or both. For smaller installations, you can install a Brightmail Scanner on the same computer as your Brightmail Control Center.

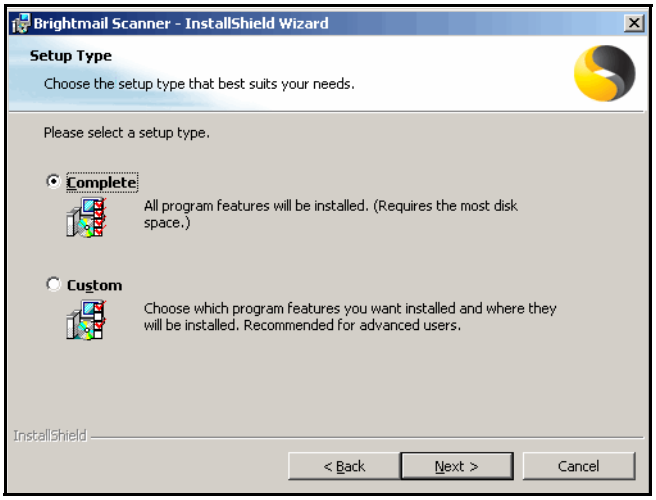
3 Click **Brightmail Scanner**.


Brightmail Scanner - InstallShield Wizard
Welcome to the InstallShield Wizard for the Brightmail Scanner
The InstallShield(R) Wizard will install the Brightmail Scanner on your computer. To continue, click Next.
WARNING: This program is protected by copyright law and international treaties.
< Back
Next >
Cancel

4 Click **Next**.
The License screen is displayed.

Brightmail Scanner - InstallShield Wizard
License Agreement
Please read the following license agreement carefully.
SYMANTEC SUBSCRIPTION SOFTWARE LICENSE AGREEMENT
SYMANTEC BRIGHTMAIL ANTISPAM
SYMANTEC CORPORATION AND/OR ITS SUBSIDIARIES ("SYMANTEC") IS WILLING TO LICENSE THE SOFTWARE TO YOU AS AN INDIVIDUAL, THE COMPANY, OR THE LEGAL ENTITY THAT WILL BE UTILIZING THE SOFTWARE (REFERENCED BELOW AS "YOU" OR "YOUR") ONLY ON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS OF THIS LICENSE AGREEMENT. READ THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT CAREFULLY BEFORE USING THE SOFTWARE. THIS IS A LEGAL AND ENFORCEABLE CONTRACT BETWEEN YOU AND THE LICENSOR. BY OPENING
I accept the terms of this license agreement
I do not accept the terms of this license agreement
InstallShield
< Back
Next >
Cancel

5 After reading the license agreement, click **I accept the terms of this license agreement**, and then click **Next**.

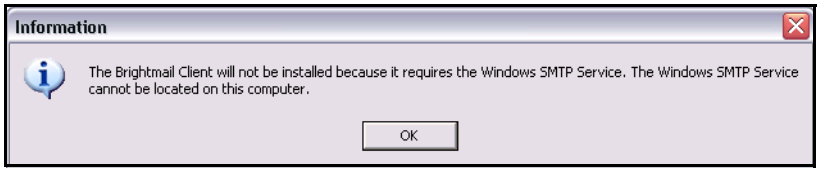

Brightmail Scanner - InstallShield Wizard
Setup Type
Choose the setup type that best suits your needs.
Please select a setup type.
Complete
All program features will be installed. (Requires the most disk space.)
Custom
Choose which program features you want installed and where they will be installed. Recommended for advanced users.
InstallShield
< Back
Next >
Cancel

6 Choose a setup type, and then click **Next**.

The **Complete** option installs all software in a predefined set of folders and files. If you are using this option, skip to Step 9. The **Custom** option allows you to tailor installation options.

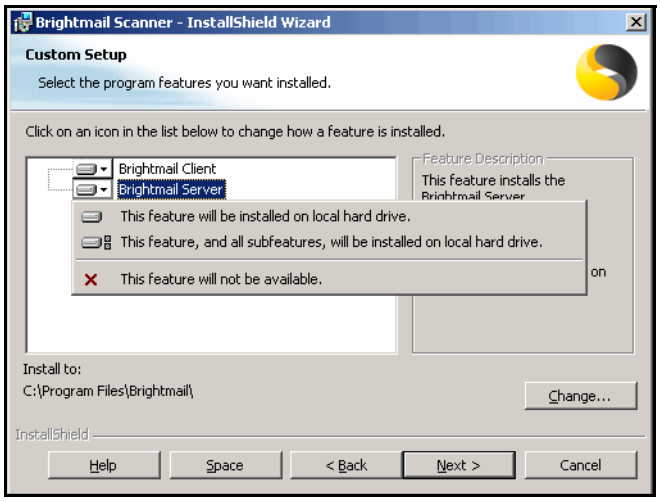
NOTE: *If you are upgrading from Version 6.0.0 or 6.0.1 to Version 6.0.2, the Installer will choose the Version 6.0.x installation folder for you and display it at the bottom of the next screen. If you choose Custom, you will be able to change the installation folder. Unless you have uninstalled the prior version,* do not change *the installation folder. See* "Upgrading Software," on page 44.

If you see the following error, either you don't have the Windows SMTP Service installed on this computer or you attempted to install the product on a non-Server version of Windows, such as Windows 2000 Professional. The Windows SMTP Service is part of Exchange 2000 and 2003.


Information
The Brightmail Client will not be installed because it requires the Windows SMTP Service. The Windows SMTP Service cannot be located on this computer.
OK

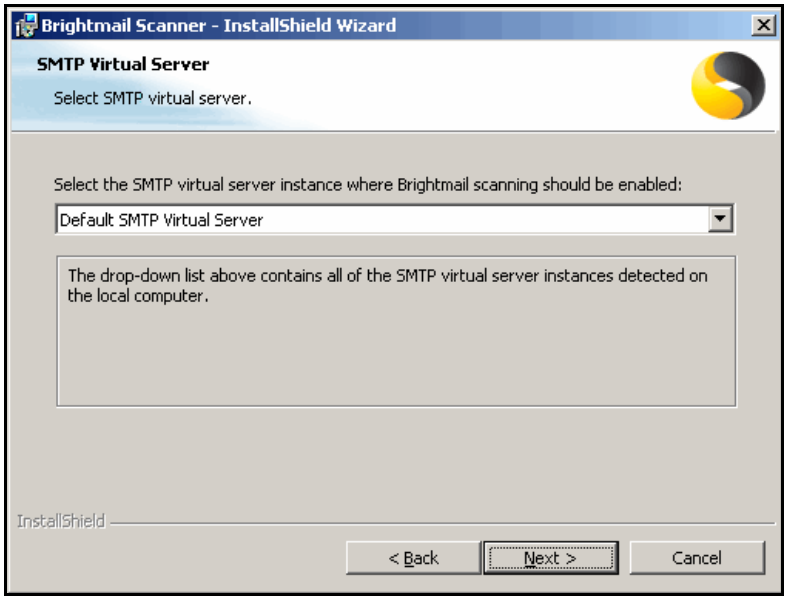
The Brightmail Client requires the Windows SMTP Service to block spam.

7 You can also, in the **Custom Setup** dialog box, click the appropriate icon to expand the list of customization options for a component

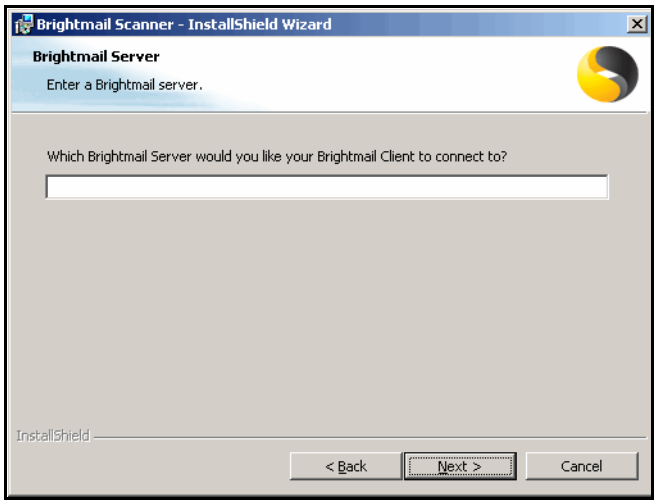

Brightmail Scanner - InstallShield Wizard
Custom Setup
Select the program features you want installed.
Click on an icon in the list below to change how a feature is installed.
Brightmail Client
Brightmail Server
Feature Description
This feature installs the
This feature will be installed on local hard drive.
This feature, and all subfeatures, will be installed on local hard drive.
This feature will not be available.
on
Install to:
C:\Program Files\Brightmail\
Change...
InstallShield
Help
Space
< Back
Next >
Cancel

Click **Space** to test your available disk space against the space requirements for the selected application; click **Change** to specify a different drive or folder for installation.

8 Make any changes you want, and then click **Next**.

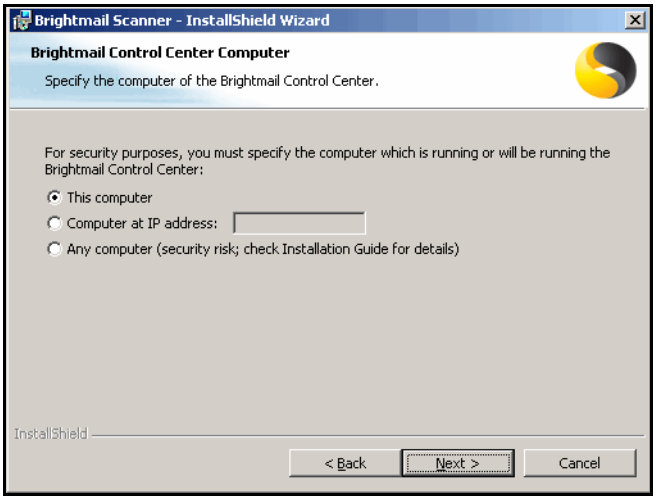

Brightmail Scanner - InstallShield Wizard
SMTP Virtual Server
Select SMTP virtual server.
Select the SMTP virtual server instance where Brightmail scanning should be enabled:
Default SMTP Virtual Server
The drop-down list above contains all of the SMTP virtual server instances detected on the local computer.
InstallShield
< Back
Next >
Cancel

9 If you are installing the Brightmail Client, select an SMTP virtual server from the drop-down list, and then click **Next**. (The dialog box above will not appear if you are only installing the Brightmail Server.)


Brightmail Scanner - InstallShield Wizard
Brightmail Server
Enter a Brightmail server.
Which Brightmail Server would you like your Brightmail Client to connect to?
InstallShield
< Back
Next >
Cancel

10 If you are installing only a Brightmail Client, you will be asked to specify a Brightmail Server.

Supply the IP address for the Brightmail Server to which you wish to connect this client. It is not necessary for the Brightmail Server to be already installed.


Brightmail Scanner - InstallShield Wizard
Brightmail Control Center Computer
Specify the computer of the Brightmail Control Center.
For security purposes, you must specify the computer which is running or will be running the Brightmail Control Center:
This computer
Computer at IP address:
Any computer (security risk; check Installation Guide for details)
InstallShield
< Back
Next >
Cancel

11 When asked for the location of your Brightmail Control Center:

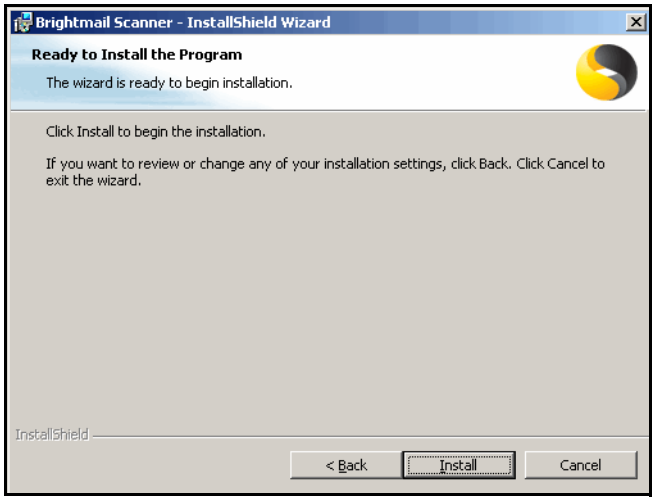
— Choose **This computer** if you are planning on a single machine installation of a Brightmail Scanner and a Brightmail Control Center

— Choose **Any computer** to allow the attachment of any computer as the Control Center for this Brightmail Scanner.

NOTE: *Depending on your network security architecture, choosing* **Any computer** *could pose a security risk, because it allows this Brightmail Scanner to be controlled from any computer that has HTTPS access to this computer.*

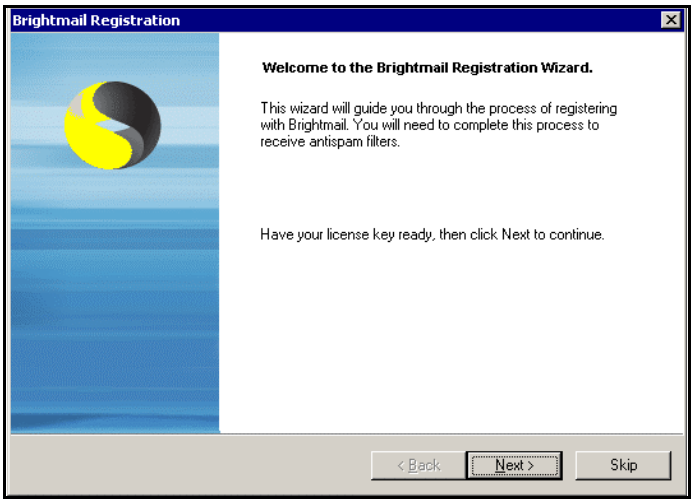
— Choose **Specify computer by IP** to allow the attachment of a different but specific computer as the Control Center for this Brightmail Scanner.

The Installer is now ready to install the Brightmail Scanner.


Brightmail Scanner - InstallShield Wizard
Ready to Install the Program
The wizard is ready to begin installation.
Click Install to begin the installation.
If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.
InstallShield
< Back
Install
Cancel

12 You can click **Back** to change or review your settings. When you are ready, click **Install** to proceed with the installation.

The Symantec software installs.

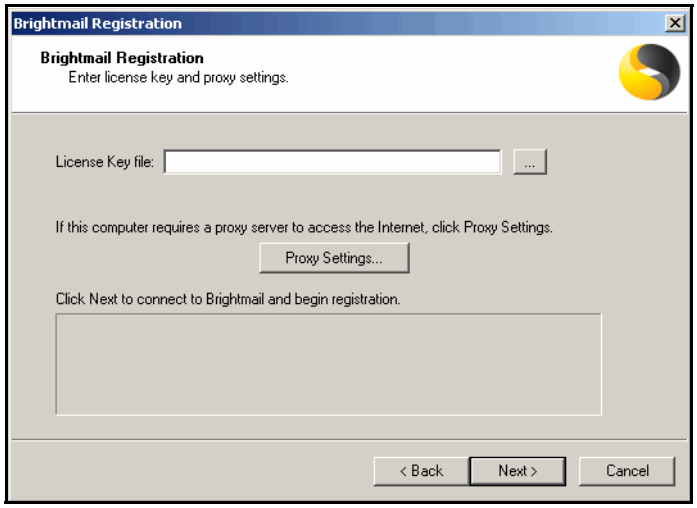

Brightmail Registration
Welcome to the Brightmail Registration Wizard.
This wizard will guide you through the process of registering with Brightmail. You will need to complete this process to receive antispam filters.
Have your license key ready, then click Next to continue.
< Back
Next >
Skip

For an installation that includes a Brightmail Server, you must register to allow Symantec Brightmail AntiSpam to receive filter updates from Symantec.

NOTE: *If you are upgrading from Version 6.0.0 or 6.0.1 to Version 6.0.2, there is no need to re-register. You will not be asked to register; the InstallShield Wizard Completed screen will appear. However, if your license key is expired, you will need to obtain an* `.slf` *file from your Symantec sales person or from* `http://www.symantecstore.com/renew` *and register after successful installation.*

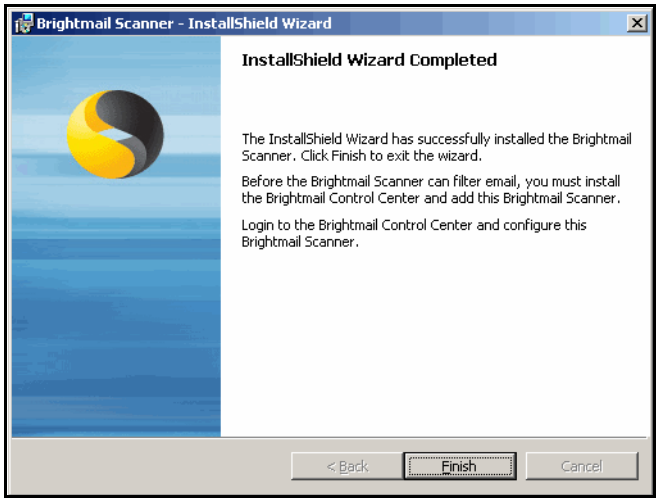
To register Brightmail Scanner:

1 Click **Next**.


Brightmail Registration
Brightmail Registration
Enter license key and proxy settings.
License Key file:
...
If this computer requires a proxy server to access the Internet, click Proxy Settings.
Proxy Settings...
Click Next to connect to Brightmail and begin registration.
< Back
Next >
Cancel

2 Type or browse to (using the button at the right) the path to your Symantec license file (`.slf`), and then click **Next**.

3 If your site requires a proxy server for HTTPS access, click **Proxy Settings** to specify the proxy server.


Brightmail Scanner - InstallShield Wizard
InstallShield Wizard Completed
The InstallShield Wizard has successfully installed the Brightmail Scanner. Click Finish to exit the wizard.
Before the Brightmail Scanner can filter email, you must install the Brightmail Control Center and add this Brightmail Scanner.
Login to the Brightmail Control Center and configure this Brightmail Scanner.
< Back
Finish
Cancel

4 Click **Finish** to exit the Registration Wizard.

5 To complete installation, click **Finish**.

6 Click **Exit** in the main installation menu, or click the appropriate button to install the spam folder agent of your choice.

See "Configuring the Spam Folder Agent," on page 93 or "Configuring the Symantec Spam Folder Agent for Domino," on page 95.

Verifying Brightmail Scanner Installation

1 Click **Start**, point to **Settings**, click **Control Panel**, and then double-click **Add/Remove Programs**. The entry **Brightmail Scanner** should be displayed in the list.

2 From the **Control Panel**, double-click **Administrative Tools**, then double-click **Services**.

If only the Brightmail Client is installed, only **Brightmail Agent** is added to the list of services. If you installed the Brightmail Server, you will also see **Brightmail Server**, **Brightmail Conduit**, **Brightmail SMTP Harvester**, and **Brightmail Virus Cleaner**.

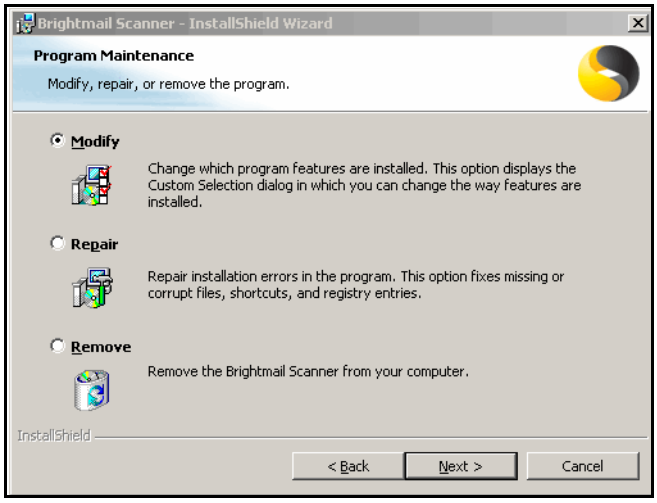
NOTE: *The Brightmail Client is not a process in Windows. It runs as part of the Windows SMTP service.*

Modifying, Repairing, and Removing Brightmail Scanner

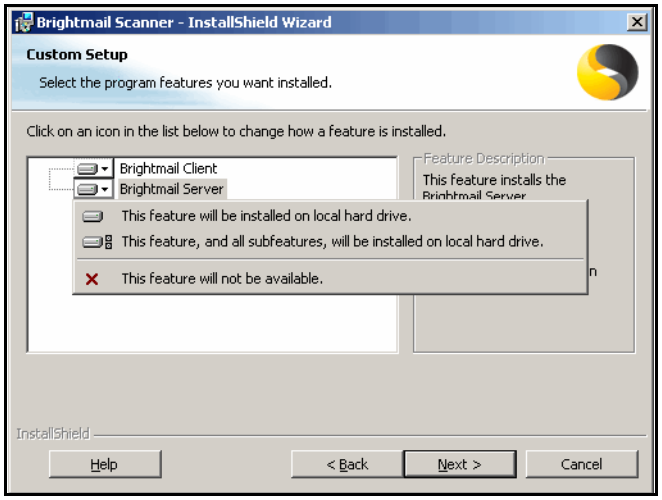
It may be necessary to modify, repair, or remove Brightmail Scanner.

To modify Brightmail Scanner:

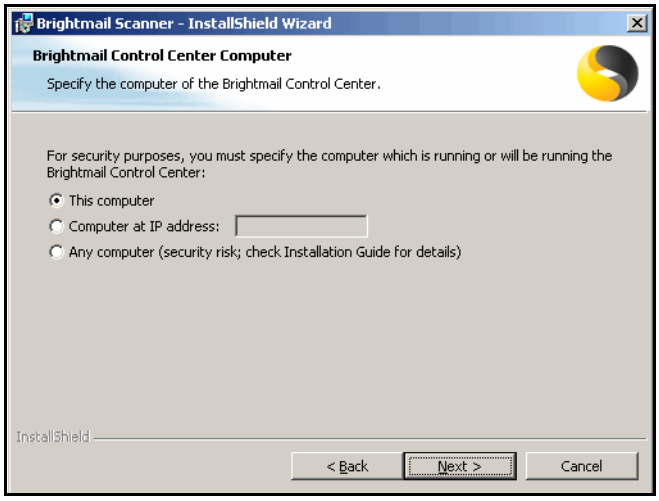
1. Click **Start**, point to **Settings**, click **Control Panel**, and then double-click **Add/ Remove Programs**.
2. Select **Brightmail Scanner** and then click **Change**.
3. Click **Next** to skip the introductory dialog box.


Brightmail Scanner - InstallShield Wizard
Program Maintenance
Modify, repair, or remove the program.
Modify
Change which program features are installed. This option displays the Custom Selection dialog in which you can change the way features are installed.
Repair
Repair installation errors in the program. This option fixes missing or corrupt files, shortcuts, and registry entries.
Remove
Remove the Brightmail Scanner from your computer.
InstallShield
< Back
Next >
Cancel

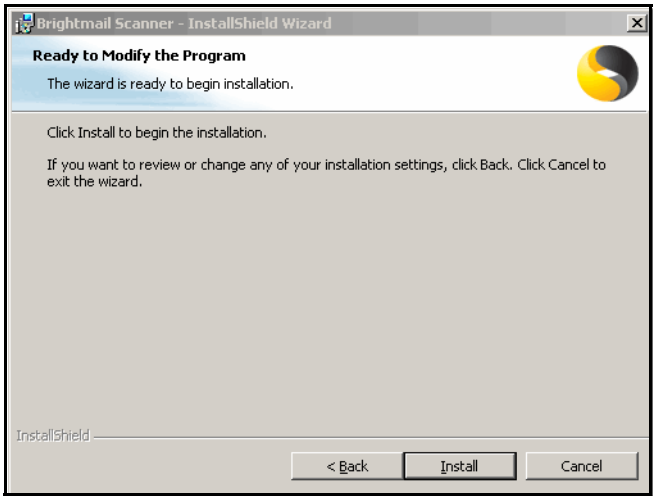
4. Click **Modify**, and then click **Next**.


Brightmail Scanner - InstallShield Wizard
Custom Setup
Select the program features you want installed.
Click on an icon in the list below to change how a feature is installed.
Brightmail Client
Brightmail Server
Feature Description
This feature installs the
This feature will be installed on local hard drive.
This feature, and all subfeatures, will be installed on local hard drive.
This feature will not be available.
InstallShield
Help
< Back
Next >
Cancel

5. Click the appropriate icon to expand the list of customization options for a component Modify components if required, and then click **Next**.


Brightmail Scanner - InstallShield Wizard
Brightmail Control Center Computer
Specify the computer of the Brightmail Control Center.
For security purposes, you must specify the computer which is running or will be running the Brightmail Control Center:
This computer
Computer at IP address:
Any computer (security risk; check Installation Guide for details)
InstallShield
< Back
Next >
Cancel

6 Indicate where your Brightmail Control Center is and click **Next.**


Brightmail Scanner - InstallShield Wizard
Ready to Modify the Program
The wizard is ready to begin installation.
Click Install to begin the installation.
If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.
InstallShield
< Back
Install
Cancel

7 Click **Install**.

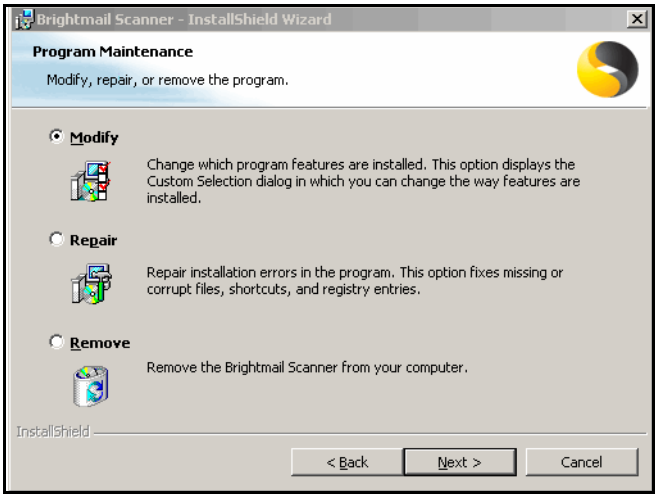
8 Click **Finish**.

To repair Brightmail Scanner:

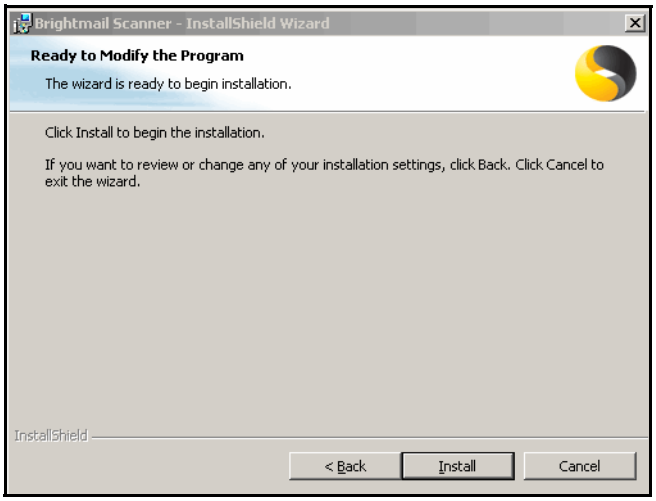
1 Click **Start**, point to **Settings**, click **Control Panel**, and then double-click **Add or Remove Programs**.

2 Select **Brightmail Scanner** and then click **Change**.

3 Click **Next** to skip the introductory dialog box.


Brightmail Scanner - InstallShield Wizard
Program Maintenance
Modify, repair, or remove the program.
Modify
Change which program features are installed. This option displays the Custom Selection dialog in which you can change the way features are installed.
Repair
Repair installation errors in the program. This option fixes missing or corrupt files, shortcuts, and registry entries.
Remove
Remove the Brightmail Scanner from your computer.
InstallShield
< Back
Next >
Cancel

4 Click **Repair**, and then click **Next**.


Brightmail Scanner - InstallShield Wizard
Ready to Modify the Program
The wizard is ready to begin installation.
Click Install to begin the installation.
If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.
InstallShield
< Back
Install
Cancel

5 Click **Install** to reinstall Symantec Brightmail AntiSpam.

6 Click **Finish**.

To remove Brightmail Scanner from your computer:

1 Click **Start**, point to **Programs**, click **Symantec Brightmail Anti-Spam**, and then click **Uninstall Brightmail Scanner**.

2 Click **Yes** to confirm uninstallation.

Installing Brightmail Control Center

The Brightmail Control Center is a Web-based cross-platform configuration and administration center built in Java. Each Symantec Brightmail AntiSpam installation has one Brightmail Control Center, which also houses Brightmail Quarantine and supporting software. You can configure and monitor all of your Brightmail Scanners from the Control Center. This section describes the environment needed to install a Brightmail Control Center, and gives a step-by-step guide for installation.

The following major sections are included:

- Hardware Requirements
- Software Environment Requirements
- Upgrading Software
- Installing Brightmail Control Center on UNIX
- Installing Brightmail Control Center on Windows
- Automatic Startup Configured by Brightmail Control Center Installer
- Uninstalling Brightmail Control Center on UNIX
- Uninstalling Brightmail Control Center on Windows

NOTE: *If you are upgrading from Version 6.0.0 or 6.0.1, refer to* "Upgrading Software," on page 60.

Hardware Requirements

The Brightmail Control Center requires the following minimum hardware setup:

- Solaris
  - UltraSPARC processor
  - 512 MB RAM minimum (1 GB or more recommended)
  - 250 MB disk space minimum (1 GB or more recommended)
- Linux or Windows
  - Intel Pentium or compatible III or IV processor
  - 512 MB RAM minimum (1 GB or more recommended)
  - 250 MB disk space minimum (1 GB or more recommended)

For more information on hardware requirements, see the *Symantec Brightmail AntiSpam Deployment Planning Guide*.

Software Environment Requirements

Listed below are the requirements for installing a Brightmail Control Center.

- **Root access** using `su` or `sudo` (on UNIX only)
- **GNU tar** (on Solaris only) Because the tar file names exceed the 40 character file name limit of native Solaris tar, GNU tar is required to install Symantec Brightmail AntiSpam. GNU tar for Solaris is available from `http://www.sunfreeware.com` and other web sites.
- **MySQL User and Group definitions (UNIX only)**

  If you are using the MySQL database packaged with the Brightmail Control Center, create a UNIX user called mysql in a group called mysql before installing the Brightmail Control Center on Linux or Solaris. If you don't, the Installer won't be able to start the MySQL daemon. No special permissions are required for the mysql user or group.

  To create this user and group on Solaris:

```
$ su
Password: your_root_password
# groupadd mysql
# useradd -c "MySQL user" -g mysql mysql
```

  To create this user and group on Linux:

```
$ su
Password: your_root_password
# groupadd -r mysql
# useradd -c "MySQL user" -r -g mysql mysql
```

- **82 MB of free disk space** for the installed files
- **230 MB of free `/tmp` disk space** for use during installation (UNIX only)

  You can set the environment variable `IATEMPDIR` to an alternate temporary storage directory if your `/tmp` directory does not have enough space.

```
$ IATEMPDIR=directory_name
```

- **Only one installation of Control Center** per customer.

Operating System Compatibility

The Control Center runs on the following operating systems:

- Microsoft Windows 2000 Server (SP2), Windows 2000 Advanced Server, or Windows Server 2003
- Red Hat Enterprise Linux AS 3.0

  Red Hat Enterprise Linux ES 3.0

  For Linux installations, the Installer requires the `compat-libstdc++` library. The `compat-libstdc++` library is available on your Red Hat distribution CD.
- Sun Solaris 8 or 9

  For Solaris 8, patch 112438 is required.

LDAP Compatibility for Brightmail Quarantine

Unless configured for administrator-only access, Brightmail Quarantine requires an LDAP server to authenticate users as they log in to access their quarantined messages and to allow Quarantine to expand user mail aliases. The following LDAP servers are compatible with Brightmail Quarantine:

- Active Directory (all versions)
- Netscape/iPlanet Directory Server 4.2 and 5.1
- Sun ONE Directory Server 5.2
- Exchange 5.5

You should be familiar with the particular LDAP schema used at your company.

Web Browser Compatibility

The Brightmail Control Center can be accessed using the following browsers:

- Internet Explorer 6.0 and greater
- Netscape 7.1 and greater

NOTE: *If your computer already has Netscape 7.1 and you plan to use Netscape 7.1, you must download and install a new copy of Netscape 7.1. Symantec Brightmail AntiSpam reports will export correctly only with the latest available copies of Netscape 7.1.*

Checking for Port Availability Via TCP/IP

Table 4 lists the ports used by the Brightmail Control Center. Other computers on your network should be able to access these ports, such as the computer where Brightmail Scanner is installed.

Table 4. Ports Used by the Brightmail Control Center

Port Number	Purpose
41025	Brightmail Scanner sends spam email to this port using the SMTP email protocol.
41080	User and administrator Web browsers connect to Symantec software on this port by default. During installation, you can configure the system to use a different port. If you configure the Brightmail Control Center to use a different Web application server than Tomcat, the Web access port will most likely be different. For example, the port used by WebLogic is `7001`.
41443	When the Installer installs Tomcat as a part of the Brightmail Control Center installation, Tomcat is configured with a self-signed SSL certificate on a secondary port, using `https://localhost:41443/brightmail`.

Upgrading Software

You must upgrade all of your Brightmail Scanners before you upgrade your Brightmail Control Center. You can upgrade from Version 6.0.0 or Version 6.0.1. Upgrading or migrating data from Version 5.5 or earlier versions is not supported. Use of the **Settings** > **Migration** page in the Brightmail Control Center is not supported.

Follow the instructions for a new installation, and note the following:

- For a UNIX installation, before starting the installation, stop Tomcat. You can use the following command, as root, to stop Tomcat:

```
# `/etc/init.d/tomcat4 stop`
```

- Some of the screens depicted for a new installation will not appear.
- It is crucial that you upgrade all of your Brightmail Scanners before you upgrade your Brightmail Control Center. Before proceeding, review the information in either "Upgrading Software," on page 44 for Windows Brightmail Scanners, or "Upgrading Software," on page 21 for UNIX Brightmail Scanners.

Installing Brightmail Control Center on UNIX

This section describes how to install the Brightmail Control Center on Linux and Solaris.

Accessing the UNIX Install Script

An install script has been prepared for Linux and Solaris installations of the Brightmail Control Center. The install script provides the appropriate Java runtime environment for the Installer.

To locate the Install script:

1 Do one of the following to navigate to the install script based on whether you are installing from a CD-ROM or a downloaded file:

If you are installing from a CD-ROM:

a. Insert the CD containing Symantec Brightmail AntiSpam software into the CD-ROM drive. The CD will mount automatically to `/cdrom/bas_60x` on Solaris systems.

b. If you are using Linux, mount the CD-ROM.

```
$ mount /dev/cdrom
```

This command can fail if you've modified `/etc/fstab` on your system.

c. If you are using Linux, type:

```
$ cd /mnt/cdrom
```

d. Change to the appropriate directory for your CD-ROM.

```
$ cd operating_system
```

You will see the following top-level directories and files:

Table 5. Linux/Solaris Directories and Files for Brightmail Control Center Installation

File or Directory	Contents
`EULA`	File containing the End User License Agreement
`install`	Install script to prepare system and run the Installer
`bcc_install_`*`platform`*`.bin`	Installer binary for Solaris or Linux, invoked by the `install` script
`documentation`	List of available documentation

e. Locate the two files, `install` and `EULA`.

If you are installing from a downloaded tar file:

a. Change to the directory that contains the Symantec Brightmail AntiSpam software.

b. Uncompress and untar the distribution file.

```
For Solaris:
$ tar -zxvf BAS_60x_sparc_solaris.tgz
```

```
For Linux:
$ tar -zxvf BAS_60x_x86_linux.tgz
```

c. Locate the two files, `install` and `EULA`.

2 Open and read the file named `EULA`.
You must read this End User License Agreement before performing the installation.

3 If you are using a previous version, read the next section. If not, continue with "Running the Installer on UNIX," on page 62.

Running the Installer on UNIX

NOTE: *If you are upgrading to Version 6.0.2, see* "Upgrading Software," on page 60 *before proceeding.*

Table 6 describes the ways to invoke the Installer when installing Brightmail Control Center.

Table 6. Installer Invocation Methods

Method	Command	Description
Command Line	`install`	The Installer prompts are presented in the terminal window in which you started the Installer.
Graphical User Interface (GUI)	`install -i awt`	The Installer prompts are presented using X Windows. To use this GUI installation, X Windows must be installed and configured correctly on your system.

The prompts for the command line and GUI installation are the same. Only the command line installation is presented in this guide.

NOTE: *When running on Red Hat Enterprise Linux, the Installer requires the presence of the* `compat-libstdc++` *library. If this library is not on your machine, the Installer will stop and ask you to install the library before you install Control Center. The* `compat-libstdc++` *library is available on your Red Hat distribution CD.*

NOTE: *If you plan to install the Brightmail Control Center in the same directory in which Brightmail Quarantine is installed, manually turn off the Tomcat Web Application server.*

1 As `root` user, run the Installer:

```
$ su root -c './install'
Password: your_root_password
```

If you have binaries in the same directory for the Brightmail Control Center and Brightmail Scanner, you will see the following:

```
Installers for both Brightmail Control Center and Brightmail
Scanner software are present and available to be installed.
Please select one of the following:
        1 -     Brightmail Scanner
        2 -     Brightmail Control Center
        q -     Quit or Exit
Which software would you like to install? 2
```

2 When necessary, choose `2` from the menu and press Enter to install the Brightmail Control Center.

The install script runs, prepares your system as required, and then runs the Installer. The Installer displays introductory text.

```
Introduction
------------

The Installer will guide you through the installation of Brightmail
   Control Center, part of Symantec Brightmail AntiSpam.

Respond to each prompt to proceed to the next step in the
   installation.  If you want to change something on a previous step,
   type 'back'.

You may cancel this installation at any time by typing 'quit'.

PRESS <ENTER> TO CONTINUE:
```

3 Press **Enter**.

The following text is displayed:

```
Get User Input: License Agreement
-----------------

Do you agree to the terms and conditions covered in the license
   agreement: /directory_path/EULA ?

    1- Yes
  ->2- No

ENTER THE NUMBER FOR YOUR CHOICE, OR PRESS <ENTER> TO ACCEPT THE
   DEFAULT:
    : 1
```

4 Read the License Agreement, if you have not already done so, and indicate whether or not you accept it as provided. To accept the licensing agreement, type `1`.

The following text is displayed:

```
Choose Install Folder
---------------------

Where would you like to install the Brightmail Control Center?
  Default Install Folder: /opt/symantec/sbas/ControlCenter

ENTER AN ABSOLUTE PATH, OR PRESS <ENTER> TO ACCEPT THE DEFAULT
      :
```

5 Choose the installation directory—the path to the Brightmail Control Center files. To accept the recommended path, press Enter.

NOTE: *If you choose to enter information at this prompt, be very careful not to insert any spaces as you type. Spaces are not stripped from input that you enter, and they can cause the installation to fail.*

NOTE: *While acceptable, setting the location of the installation directory to a remotely mounted partition is not recommended. If you do so, the Installer issues a warning and prompts you to set it to a local partition.*

The following text is displayed:

```
Web Application Server
The Brightmail Control Center requires a Web application server.

Would you like to install the included copy of Tomcat version 4.1.27
   server as your Web Application server, or use your own Web
   Application server?

  ->1- Install included copy of Tomcat
    2- Use my own Web Application server

ENTER THE NUMBER FOR YOUR CHOICE, OR PRESS <ENTER> TO ACCEPT THE
   DEFAULT:
    :
```

6 Select `1` to install the included Tomcat server or `2` to use your own Web Application server. The Brightmail Control Center requires a Web Application server. The Tomcat Web Application server is bundled and automatically installed with the Brightmail Control Center. Tomcat and WebLogic are the only Web Application servers tested to work with the Brightmail Control Center. For information on using your own Web application server, refer to "Configuring the Brightmail Control Center to Use WebLogic," on page 81.

If you are using Tomcat, the following text is displayed:

```
Tomcat Port
-----------

You have chosen to install the included copy of Tomcat as your
Web Application Server. Please specify the port number where you
will be running the Tomcat Server.

Tomcat port number (DEFAULT: 41080):
```

7 Press Enter to select the default port address of `41080`, or you can enter a different port address.

NOTE: *The Installer configures Tomcat with a self-signed SSL certificate on a secondary port, using* `https://localhost:41443/brightmail`.

If you have set the MySQL user and group as described previously, the Installer now proceeds to the Pre-Installation Summary screen. Otherwise, the Installer displays an error and exits.

A summary of the choices you've made is displayed.

```
Pre-Installation Summary
------------------------

Please Review the Following Before Continuing:

Product Name:
    Brightmail Control Center

Install Folder:
     /opt/symantec/sbas/ControlCenter

Application Server:
    Tomcat


PRESS <ENTER> TO CONTINUE:
```

8 Press Enter to continue based on these settings.

Before proceeding to installation, the Installer checks to see if Brightmail Quarantine exists on the machine on which you are currently installing Brightmail Control Center. If no earlier version of Quarantine is detected, the Installer asks you where to install the Brightmail Control Center. If an earlier version of Quarantine is detected, Quarantine data is automatically migrated to Version 6.0.2, using the same location. This may take a few minutes.

Next, `Installing...` appears on the screen, and a progress bar is displayed.

```
Installing...
-------------


[================|================|================|==============]
[----------------|--------
```

9 When installation is complete, one of the following two messages is displayed, depending on the choice you made regarding your Web Application server:

```
Installation Complete
---------------------

The Brightmail Control Center installation has been completed.

You chose to install the included copy of Tomcat, you can access the
Brightmail Control Center here:
http://localhost:41080/brightmail

Login with:
Username: admin
Password: symantec

If you are upgrading from a previous version, use your existing password
instead.

Click 'Exit' to exit the installer.

PRESS <ENTER> TO EXIT THE INSTALLER:
```

```
Installation Complete
---------------------

The Brightmail Control Center installation has been completed.

You chose to install your own Web Application Server, see the
Symantec Brightmail AntiSpam Installation Guide for instructions.

Click 'Exit' to exit the installer.

PRESS <ENTER> TO EXIT THE INSTALLER:
```

For additional information on accessing the Brightmail Control Center, see "Logging in and Logging out," on page 76.

Reinstalling Control Center on UNIX

The Installer can re-install your current software and preserve existing configuration and other data stored after initial installation. One of the following actions is taken when a Symantec software installation is detected:

- **No version of Control Center is found –** Installation occurs normally.
- **Brightmail Control Center exists –** The Installer reinstalls your existing software, in the same location as the previous version. If current versions of MySQL and Tomcat exist, they are not reinstalled. Except for the MySQL and Tomcat files, all Control Center binaries are updated.

Installing Brightmail Control Center on Windows

NOTE: *If you are upgrading to Version 6.0.2, see* "Upgrading Software," on page 60 *before proceeding.*

1. Close all open applications before installing Control Center.
2. Do one of the following to navigate to the **Setup.exe** file:

   If you are installing from a CD-ROM:

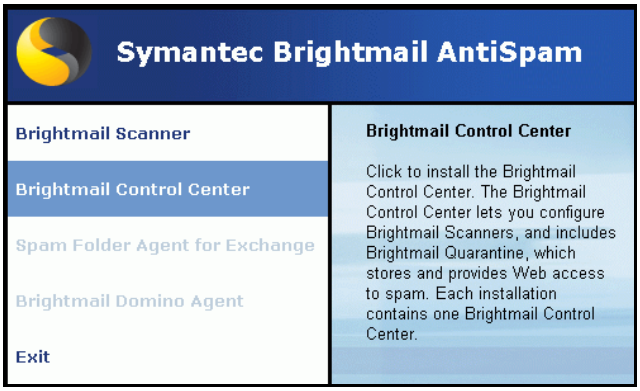
   Insert the Symantec Brightmail AntiSpam software distribution CD-ROM in your computer's CD-ROM drive.

   If the Installer does not run automatically, open the **Windows** folder on the CD using Windows Explorer and double-click the **Setup.exe** icon.

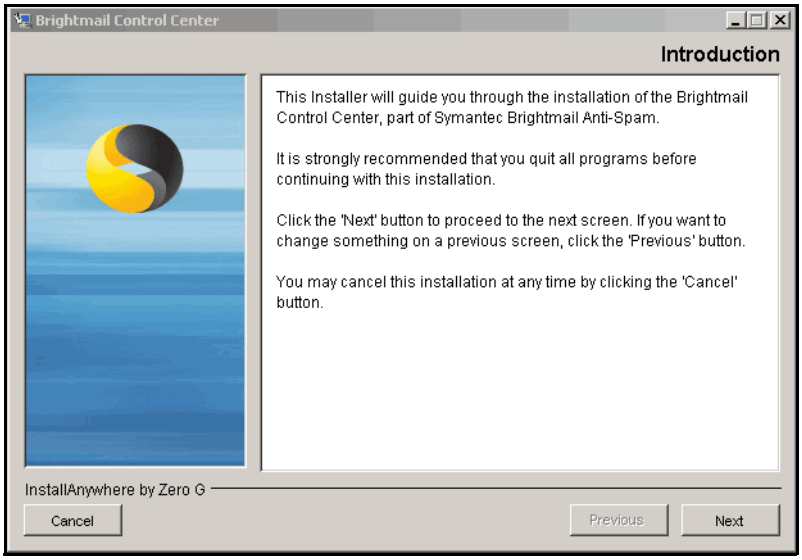
   If you are installing from a downloaded zip file:

   a. Unzip the zip file.

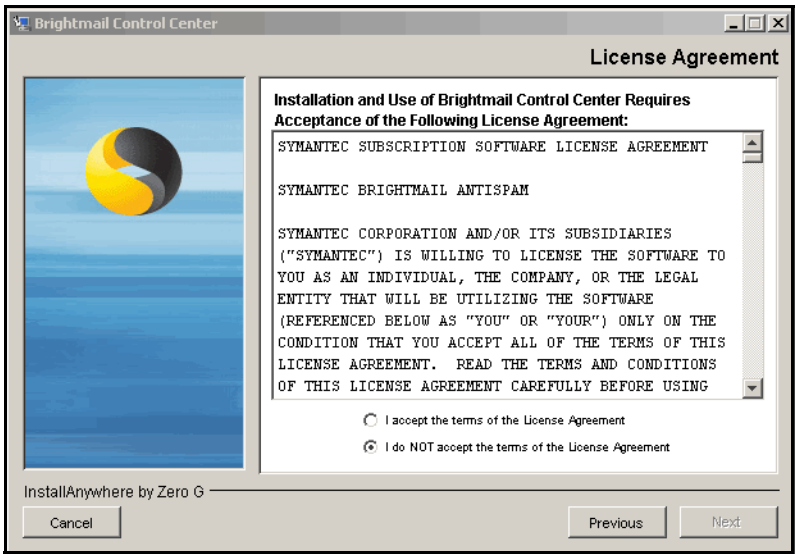
   b. Double-click the **Setup.exe** icon.


Symantec Brightmail AntiSpam
Brightmail Scanner
Brightmail Control Center
Spam Folder Agent for Exchange
Brightmail Domino Agent
Exit
Brightmail Control Center
Click to install the Brightmail Control Center. The Brightmail Control Center lets you configure Brightmail Scanners, and includes Brightmail Quarantine, which stores and provides Web access to spam. Each installation contains one Brightmail Control Center.

3. Click **Brightmail Control Center**.


Brightmail Control Center
Introduction
This Installer will guide you through the installation of the Brightmail Control Center, part of Symantec Brightmail Anti-Spam.
It is strongly recommended that you quit all programs before continuing with this installation.
Click the 'Next' button to proceed to the next screen. If you want to change something on a previous screen, click the 'Previous' button.
You may cancel this installation at any time by clicking the 'Cancel' button.
InstallAnywhere by Zero G
Cancel
Previous
Next

4 Click **Next**.


Brightmail Control Center
License Agreement
Installation and Use of Brightmail Control Center Requires Acceptance of the Following License Agreement:
SYMANTEC SUBSCRIPTION SOFTWARE LICENSE AGREEMENT
SYMANTEC BRIGHTMAIL ANTISPAM
SYMANTEC CORPORATION AND/OR ITS SUBSIDIARIES ("SYMANTEC") IS WILLING TO LICENSE THE SOFTWARE TO YOU AS AN INDIVIDUAL, THE COMPANY, OR THE LEGAL ENTITY THAT WILL BE UTILIZING THE SOFTWARE (REFERENCED BELOW AS "YOU" OR "YOUR") ONLY ON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS OF THIS LICENSE AGREEMENT. READ THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT CAREFULLY BEFORE USING
I accept the terms of the License Agreement
I do NOT accept the terms of the License Agreement
InstallAnywhere by Zero G
Cancel
Previous
Next

5 After reading the license agreement, click **I accept the Terms of the License Agreement** and then **Next**.

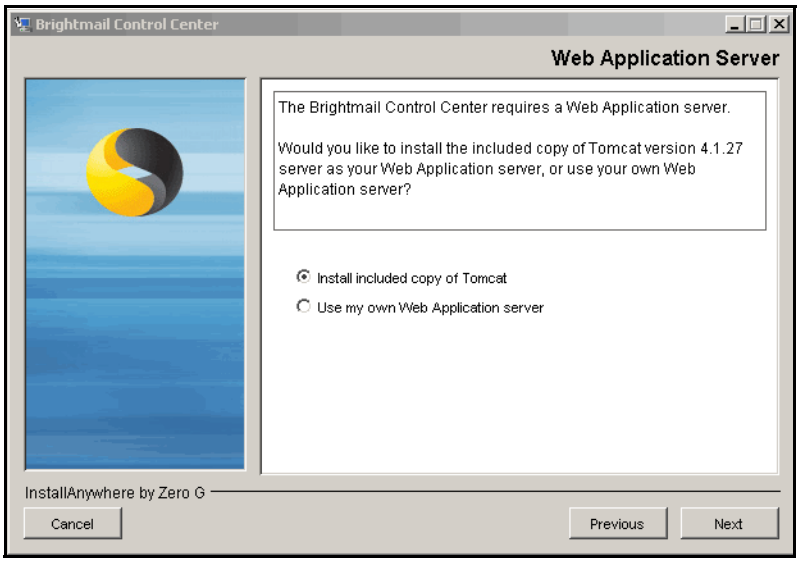
6 Click **Next** to choose the default folder for the Brightmail Control Center or click **Choose...** to select a different folder for Control Center.

NOTE: *If you are upgrading from Version 6.0.0 or 6.0.1, you will not see the screen above, as well as some of the following screens.*

The Control Center requires a Web application server. The Tomcat application server is bundled with the installation.

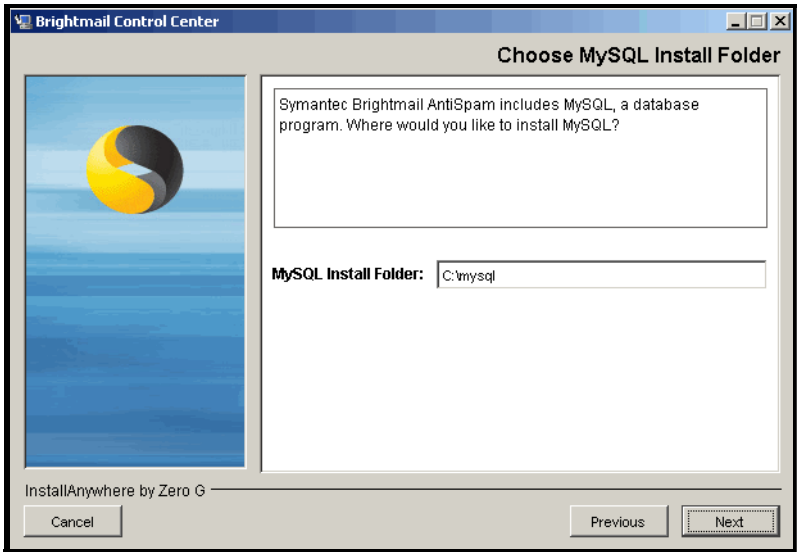
7 Do one of the following:

— Click **Install included copy of Tomcat** and click **Next**, then click **Next** to accept the default port address of `41080`, or enter a different port address.


Brightmail Control Center
Web Application Server
The Brightmail Control Center requires a Web Application server.
Would you like to install the included copy of Tomcat version 4.1.27 server as your Web Application server, or use your own Web Application server?
Install included copy of Tomcat
Use my own Web Application server
InstallAnywhere by Zero G
Cancel
Previous
Next

— Click **Use my own Web Application server**, and then click **Next**. Tomcat and WebLogic are the only web application servers tested to work with the Brightmail Control Center. For information on using your own Web application server, refer to "Configuring the Brightmail Control Center to Use WebLogic," on page 81.

NOTE: *The Installer configures Tomcat with a self-signed SSL certificate on a secondary port, using* `https://localhost:41443/brightmail`.

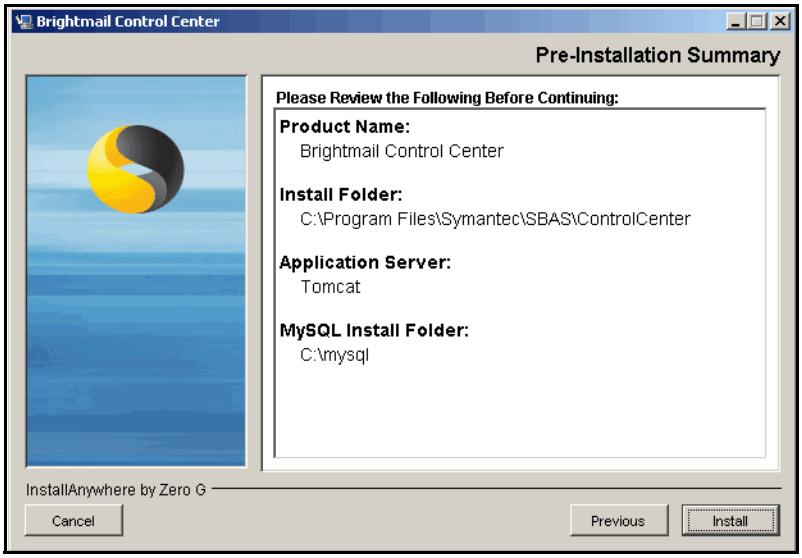


The default location for MySQL is `C:\mysql`.

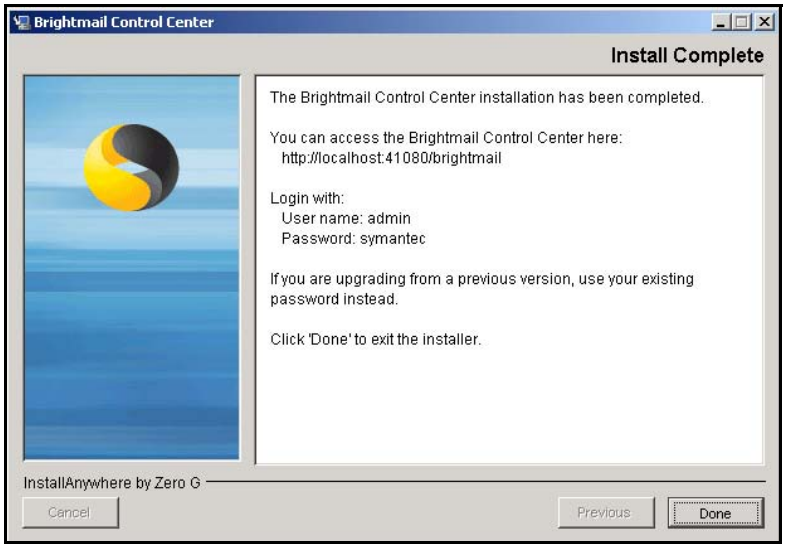
8 If you wish to install MySQL in an alternate location, enter that location here.

NOTE: *If you choose to install MySQL in an alternate location, please be aware of the following: Symantec does not recommend that you install MySQL on a networked drive as it will impact performance of the Brightmail Control Center. If you choose to do this, you must also perform some post installation configuration to allow services to run on networked drives. Do this if only you understand Windows permissions very well.*

9 Click **Next** to view the pre-installation summary.



10 When you are ready, click **Install** to proceed. The installation occurs, and when it is done the following displays:



11 Click **Done**.

12 Click **Exit** to quit from the Brightmail Control Center Installer.

Automatic Startup Configured by Brightmail Control Center Installer

Table 7 describes the processes that make up the Brightmail Control Center. The Installer configures the MySQL and Tomcat (if installed) processes to start automatically when the computer is powered up. If used immediately after installation, these processes may require 15-60 seconds to begin.

Table 7. Control Center Processes/Services

Process Name in UNIX	Service Name in Windows	Description
`java`	Tomcat	Tomcat Java servlet container—serves the pages that make up the Brightmail Control Center.
`mysqld`	MySql	MySQL server—processes requests to retrieve and store data in the MySQL database, such as Brightmail Scanner configuration data or quarantined spam messages.

On UNIX, the processes making up the Brightmail Control Center are configured to run as daemons. Startup scripts are installed in `/etc/init.d` and links are created in the appropriate `/etc/rc*` directory.

On Windows, the services making up the Brightmail Control Center are configured to a startup type of *Automatic*.

Uninstalling Brightmail Control Center on UNIX

The Uninstaller uninstalls the Brightmail Control Center files and also the MySQL and Tomcat files if they exist. Just as with the Installer, you can run the Uninstaller using the `-i awt` option described in Table 6, “Installer Invocation Methods,” on page 62.

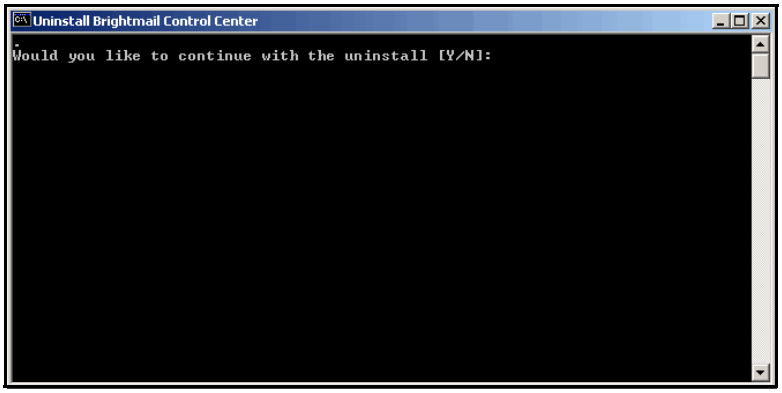
To remove Symantec software, run the Uninstaller as the root user:

```
$ su root -c '/opt/symantec/sbas/ControlCenter/uninstall.sh'
Password: your_root_password
```

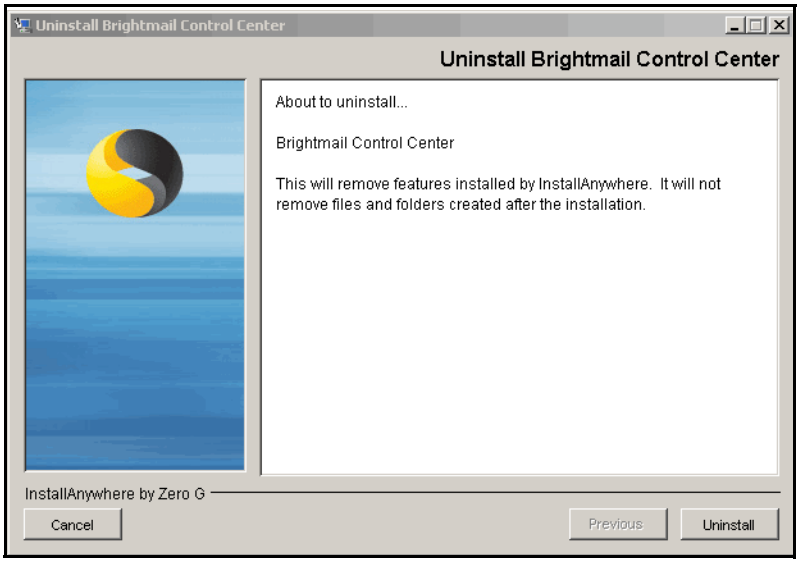
Uninstalling Brightmail Control Center on Windows

The Uninstaller removes the MySQL and Tomcat services if they exist, and then uninstalls the Brightmail Control Center files and also the MySQL and Tomcat files if they exist.

1. Click **Start**, point to **Programs**, point to **Symantec Brightmail AntiSpam**, and then click **Uninstall Brightmail Control Center**.
2. A DOS window opens and prompts you to confirm uninstallation.



3 Type **Y** and press Enter. MySQL and Tomcat are removed, then the Brightmail Control Center Uninstall screen opens in a separate window.


Uninstall Brightmail Control Center
Uninstall Brightmail Control Center
About to uninstall...
Brightmail Control Center
This will remove features installed by InstallAnywhere. It will not remove files and folders created after the installation.
InstallAnywhere by Zero G
Cancel
Previous
Uninstall

4 Click **Uninstall** to start the uninstallation process.

The Install Complete page displays. The page may list some files that it could not remove.

Control Center Testing and Configuration

This section provides initial testing procedures and instructions for system setup tasks you may need to perform. The following major topics are included:

- Testing Installation of the Brightmail Control Center
- Adding a Brightmail Scanner
- Testing Symantec Brightmail AntiSpam Filtering
- Configuring the Brightmail Control Center to Use WebLogic

Testing Installation of the Brightmail Control Center

The following sections describe how to verify that the Brightmail Control Center is installed correctly and test basic functions of Symantec Brightmail AntiSpam. You can perform the following procedures regardless of any LDAP requirements you may have for Quarantine.

Reviewing the Installation Log

You may want to check the log file created by the Brightmail Installer, either to verify the installation or to diagnose any problems you encountered in running the Installer. The installation log file is different than the runtime log file, `BrightmailLog.log`.

The installation log file, called `Brightmail_Control_Center_InstallLog.log`, is located in:

- UNIX: `/opt/symantec/sbas/ControlCenter`
- Windows: `C:\Program Files\Symantec\SBAS\ControlCenter`

This file is a plain text file, viewable with a text editor such as Notepad or `vi`. The first page contains a summary of the successful actions and any warnings, and nonfatal and fatal errors. The rest of the file has details about the Installer's actions.

Logging in and Logging out

Use the following procedures to login and logout of the Brightmail Control Center.

To Login to the Brightmail Control Center:

1. Open a browser window.

   NOTE: *In the following step, port* `41080` *is typical for the Tomcat Web application server. Other Web application servers will use different ports. For example, for WebLogic, specify port* `7001`.

2. Go to the Brightmail Control Center Login page:
   `http://localhost:41080/brightmail/`
3. Enter the desired account information, and then click **Login**.

Logging Out

To log out at any time, click the **Log Out** icon

in the upper right corner of the current screen.

Checking Versions

If problems arise with your installation, you may be asked for the versions of some products on your system.

To check the versions of your installed software:

go to `http://localhost:`*`port`*`/brightmail/BrightmailVersion`

where *`port`* is the port that Tomcat uses, typically `41080`.

You can see the installed versions of the following software:

— Brightmail Control Center or Brightmail Quarantine

— Java

— MySQL

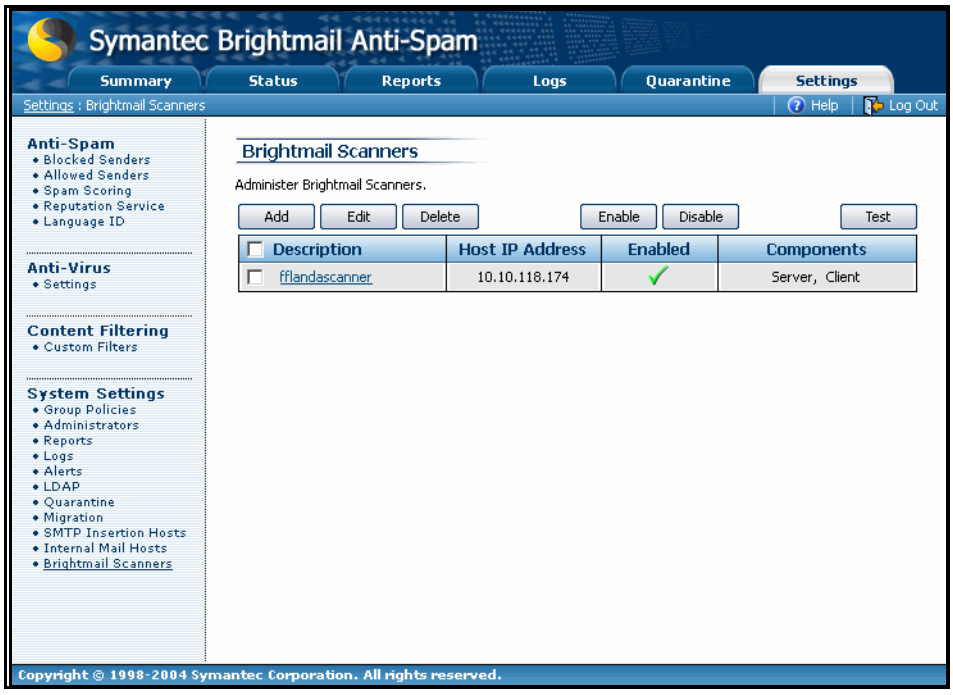
Adding a Brightmail Scanner

If this is your first time accessing the Brightmail Control Center, you must first add a Brightmail Scanner. It is assumed that before continuing, you have installed at least one Brightmail Scanner and started it, as described in "Starting a Brightmail Scanner," on page 30.

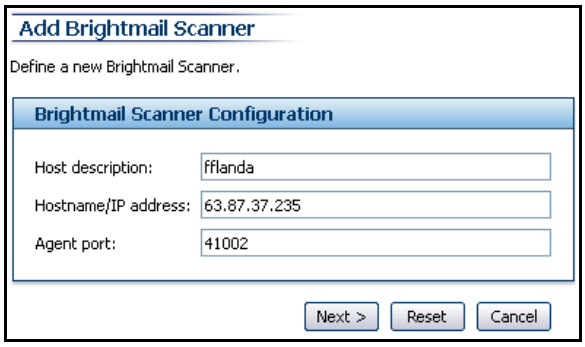
To add a Brightmail Scanner:

1 In the Brightmail Control Center, click the **Settings** tab.

2 In the left pane, under **System Settings**, click **Brightmail Scanners**.



3 On the Brightmail **Scanner Settings** page, click **Add**.



Starting a Brightmail Scanner from the Brightmail Control Center

The following steps can be used after you have initially installed and tested your installation of Symantec Brightmail AntiSpam. If you are still in the installation and testing process, be sure you have started a Brightmail Scanner as described in "Starting a Brightmail Scanner," on page 30. Once Symantec Brightmail AntiSpam is up and running, you can rely on the following steps.

To start Brightmail Scanners from the Brightmail Control Center

1. Login to your Brightmail Control Center.

   Specific steps for logging on can be found in "Logging in and Logging out," on page 76.

2. Select the **Status** tab on the Brightmail Control Center.

   You will then see one or more Brightmail Scanners displayed in a list.

3. Check the box next to the Brightmail Scanner you wish to enable. The Scanner starts automatically. The **Stop** button is now selectable.

Testing Symantec Brightmail AntiSpam Filtering

The following are sample tests by which you can verify that Symantec Brightmail AntiSpam is filtering your email as expected. Use these tests as models for additional tests you might like to perform periodically.

Verifying Normal Delivery

You can verify whether the Windows SMTP Service or Sendmail is working properly with the Brightmail Client to deliver legitimate mail by sending an email to a user.

To test delivery of legitimate mail:

1. Send an email with the subject line "Normal Delivery Test" to a user.
2. Verify that the test message arrives correctly in the normal delivery location on your local host.

Verifying Spam Filtering

This test assumes you are using default installation settings for spam message handling.

To test spam filtering with subject line modification:

1. Create a POP3 account on an email client such as Outlook Express.

   For the SMTP Server setting on this account, specify the IP address of the machine on which you have installed and started Brightmail Scanner.
2. Compose an email message addressed to an account on the machine running the Brightmail Scanner.
3. Give the message a subject that is easy to find, such as `Test Spam Message`.
4. To classify the message as spam, include the following URL on a line by itself in the message body:

   `http://www.example.com/url-1.blocked/`
5. Send the message.
6. Check the email account to which you sent the message.

   You should find a message with the same subject prefixed by the word `[Spam]`.
7. Send a message that is not spam to the same account used in step 5.
8. After several minutes have passed, in the Brightmail Control Center, click **Status** > **Overview**.

   The **Total Spam Messages** counter on the **Summary** page increases by one if filtering is working.

Testing AntiVirus Filtering

You can verify that antivirus filtering is working correctly by sending a test message containing a pseudo-infected virus. This is not a real virus.

To test the AntiVirus Cleaner:

1. Using your preferred email program, create an email message addressed to a test account.
2. Attach a virus test file such as `eicar.com` to the email.

   Virus test files are located at `http://www.eicar.org/`.
3. Send the message.
4. Check the mailbox for the test account to verify receipt of the test message with the added Cleaner message text.

Verifying Spam Filtering to Quarantine

If you've configured Symantec Brightmail AntiSpam to forward spam messages to Quarantine as described below and both the Brightmail Control Center and at least one

Brightmail Scanner is running, you should be able to see spam messages when you log into the Brightmail Control Center as an administrator. There can be a slight delay until the first spam message arrives, depending on the amount of spam received at your organization.

If new spam messages arrive for a user while that user is viewing quarantined messages, the new spam messages will be displayed after a page change. For example, if you're viewing an individual message and then return to the message list, any new messages that have just arrived will be added at the end of the message list and displayed when the last message list page is displayed.

The Brightmail Scanner must be configured to forward spam messages to Quarantine. If the default configuration is not changed, Symantec Brightmail AntiSpam inserts `[Spam]` in the subject line of spam messages and delivers them to users' normal inbox rather than Quarantine. The following Symantec Brightmail AntiSpam message categories can be configured to forward messages to Quarantine:

- Spam
- Suspected spam
- Messages from blocked senders
- Messages containing company-specific content (as defined by you)
- Messages that are unscannable for viruses

You can choose to have all, some or none of these message types forwarded to Quarantine.

NOTE: *Brightmail Quarantine only supports the ISO-Latin-1 character set. If messages are processed into the Quarantine database in other character sets, any non-compliant characters may not be readable.*

To set up delivery of messages to Quarantine:

1. In the Brightmail Control Center, click the **Settings** tab, and then click **Group Policies**.
2. Under **Groups**, click the appropriate group, such as **Default**.
3. Under AntiSpam Actions, set the filtering action to **Quarantine the Message** for the desired message types. Typically, you'll want to set **If a message is spam** or **If a message is suspected spam** to **Quarantine the Message**.
4. Click **Save**.
5. Repeat this process for each group policy that you want to set to deliver messages to Quarantine.
6. Send a spam message as described in the next procedure.

To send a message that will be classified as spam:

1. Using an email client such as Microsoft Outlook Express, open an email addressed to an account configured to filter spam to Quarantine.

2 Give the message a subject that is easy to find such as `Test Spam Message`.

3 To classify the message as spam, include one or more of the following URLs on a line by itself:

```
http://www.example.com/url-1.blocked/
http://www.example.com/URL-2.blocked/
```

4 Send the message.

5 Login to the Brightmail Control Center as an administrator and select the Quarantine tab.

6 Select the Administrator Messages List page and search for a message with the subject `Test Spam Message`.

Configuring the Brightmail Control Center to Use WebLogic

Tomcat is included with the Brightmail Control Center as the default application server. If you prefer to use the WebLogic application server with the Brightmail Control Center, follow the steps in this section.

Copying the MySQL Connector/J API

The MySQL Connector/J API is a JDBC driver for MySQL, and provides an interface between MySQL and the Java components that make up the Brightmail Control Center. If you choose to install Tomcat, the MySQL Connector/J API file is installed and configured by the Installer.

To install the MySQL Connector/J API for WebLogic:

1 On the computer where the Brightmail Control Center is installed, locate the file `mysql-connector-java-com-3.0.11-stable-bin.jar` in one of the directories below:

UNIX: `/opt/symantec/sbas/ControlCenter/brightmail`

Windows: `C:\Program Files\Symantec\SBAS\ControlCenter\brightmail`

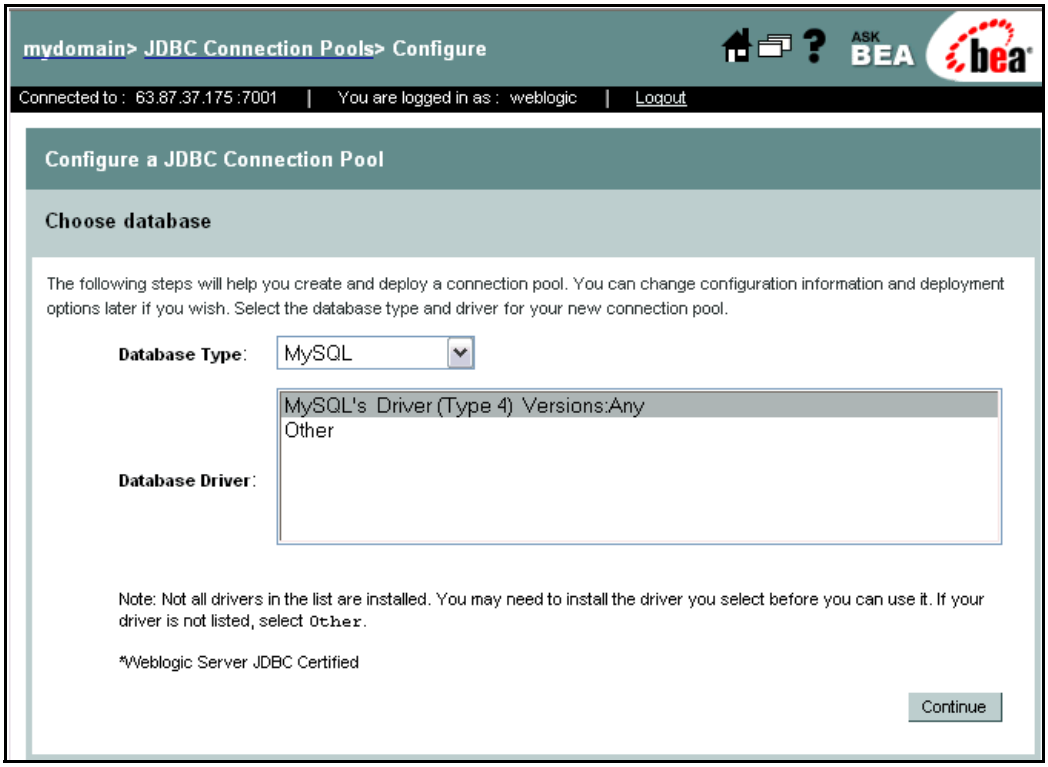
2 Copy the file `mysql-connector-java-com-3.0.11-stable-bin.jar` to an appropriate directory on the computer where WebLogic is installed. Copy the file to a directory in your CLASSPATH.

Adding MySQL Connector/J to the CLASSPATH Variable

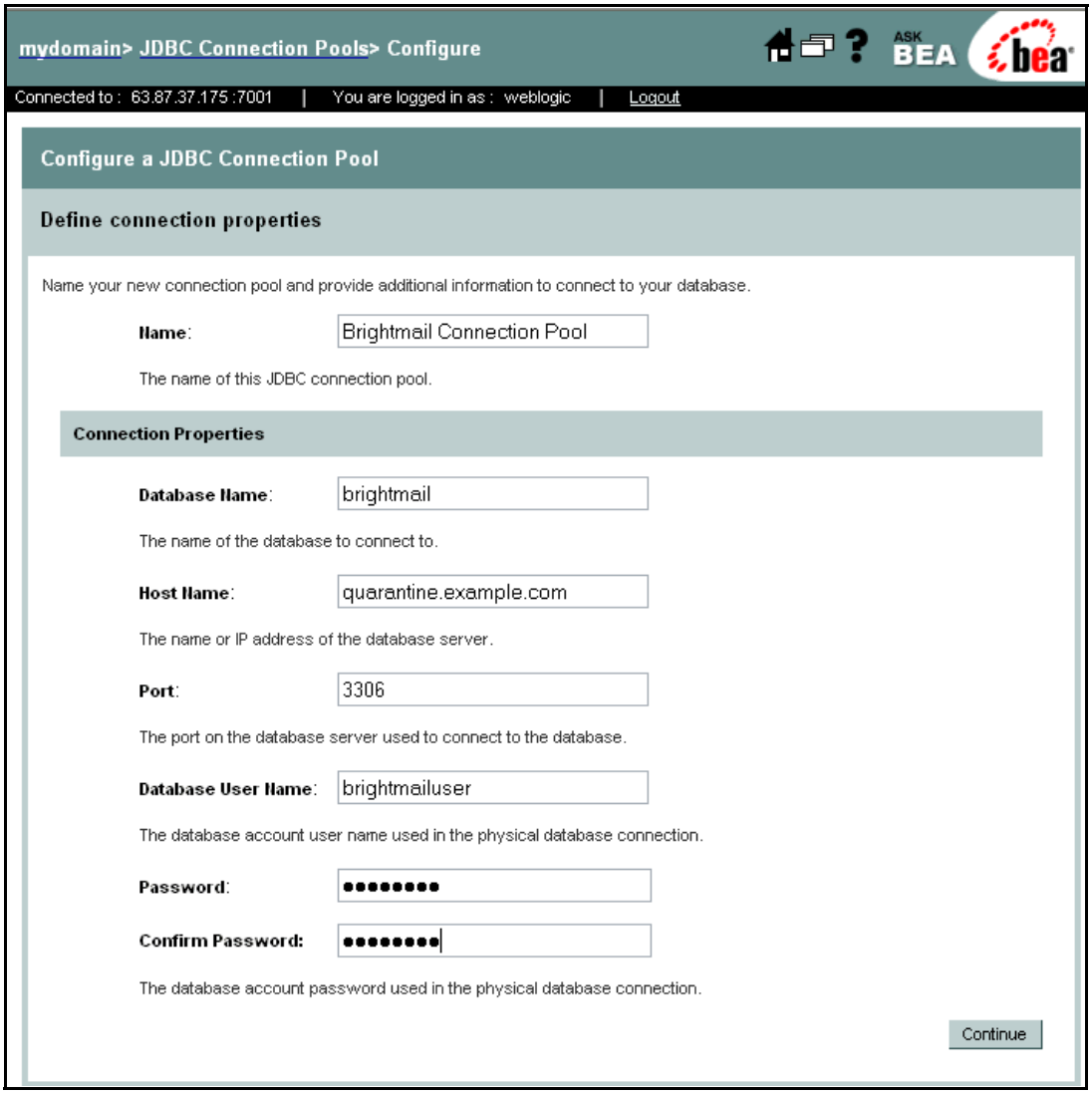
Ensure the CLASSPATH environment variable includes the MySQL Connector/J API JDBC driver file, `mysql-connector-java-com-3.0.11-stable-bin.jar` as described in the previous section. Once this `.jar` has been added to the CLASSPATH, restart your WebLogic Server, and access the WebLogic Server console.

Configuring the Brightmail JDBC Connection Pool

1. Select **JDBC Connection Pools** page in the WebLogic Server console by navigating to *your-domain*/**Services**/**JDBC**/**Connection Pools**.
2. Select **Configure a new JDBC Connection Pool…**
3. In the **Database Type** list, click **MySQL**.
4. Select the **MySQL's Driver (Type4) Versions:Any**.
   The page should appear similar to the following.


mydomain> JDBC Connection Pools> Configure
ASK BEA
Connected to : 63.87.37.175 :7001 | You are logged in as : weblogic | Logout
Configure a JDBC Connection Pool
Choose database
The following steps will help you create and deploy a connection pool. You can change configuration information and deployment options later if you wish. Select the database type and driver for your new connection pool.
Database Type:
MySQL
Database Driver:
MySQL's Driver (Type 4) Versions:Any
Other
Note: Not all drivers in the list are installed. You may need to install the driver you select before you can use it. If your driver is not listed, select Other.
*Weblogic Server JDBC Certified
Continue

5. Click **Continue**.


mydomain> JDBC Connection Pools> Configure
ASK BEA
Connected to : 63.87.37.175 :7001 | You are logged in as : weblogic | Logout
Configure a JDBC Connection Pool
Define connection properties
Name your new connection pool and provide additional information to connect to your database.
Name:
Brightmail Connection Pool
The name of this JDBC connection pool.
Connection Properties
Database Name:
brightmail
The name of the database to connect to.
Host Name:
quarantine.example.com
The name or IP address of the database server.
Port:
3306
The port on the database server used to connect to the database.
Database User Name:
brightmailuser
The database account user name used in the physical database connection.
Password:
Confirm Password:
The database account password used in the physical database connection.
Continue

6 In the **Name** box, type a name, for example `Brightmail Connection Pool`.

7 In the **Database Name** box, type `brightmail`.

8 In the **Host Name** box, type the database server's name or IP address.

9 In the **Port** box, type the port for the database server.

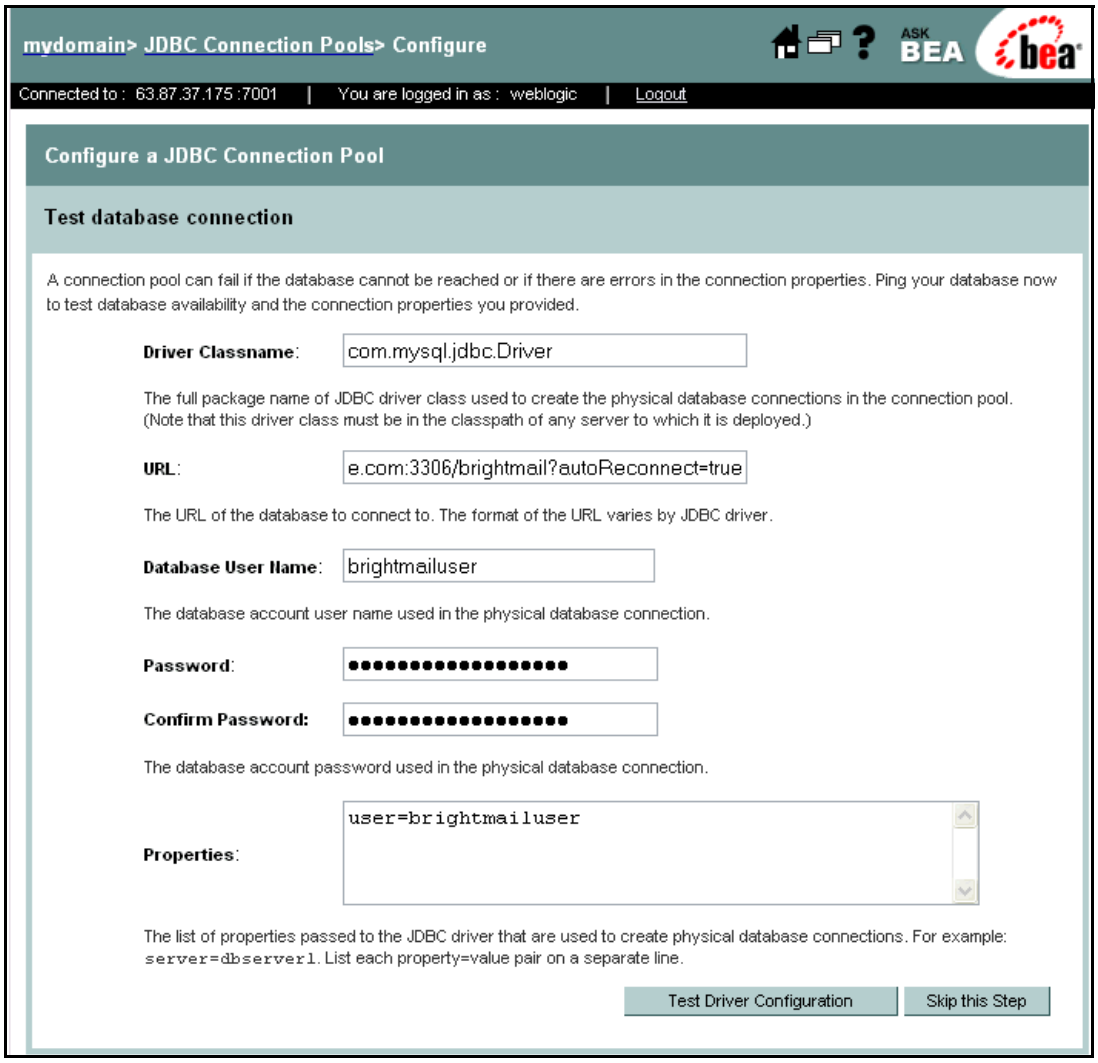
10 In the **Database User Name** box, type `brightmailuser`.

11 In the **Password** box, type `password`.

12 Confirm the password by typing in `password` again.
The page should appear similar to the picture above.

13 Click **Continue**.

The **Test database connection** page is displayed.


mydomain> JDBC Connection Pools> Configure
ASK BEA
Connected to : 63.87.37.175 :7001 | You are logged in as : weblogic | Logout
Configure a JDBC Connection Pool
Test database connection
A connection pool can fail if the database cannot be reached or if there are errors in the connection properties. Ping your database now to test database availability and the connection properties you provided.
Driver Classname: com.mysql.jdbc.Driver
The full package name of JDBC driver class used to create the physical database connections in the connection pool. (Note that this driver class must be in the classpath of any server to which it is deployed.)
URL: e.com:3306/brightmail?autoReconnect=true
The URL of the database to connect to. The format of the URL varies by JDBC driver.
Database User Name: brightmailuser
The database account user name used in the physical database connection.
Password:
Confirm Password:
The database account password used in the physical database connection.
Properties: user=brightmailuser
The list of properties passed to the JDBC driver that are used to create physical database connections. For example: server=dbserver1. List each property=value pair on a separate line.
Test Driver Configuration
Skip this Step

14 In the **Driver Classname** box, type the JDBC driver class as `com.mysql.jdbc.Driver`.

15 In the **URL** box, type the URL to the database. This has to be of the form:

`jdbc:mysql://`*`hostname:port`*`/brightmail?autoReconnect=true`.

The hostname and port number shown in italics will be the values you specified in Steps 8 and 9.

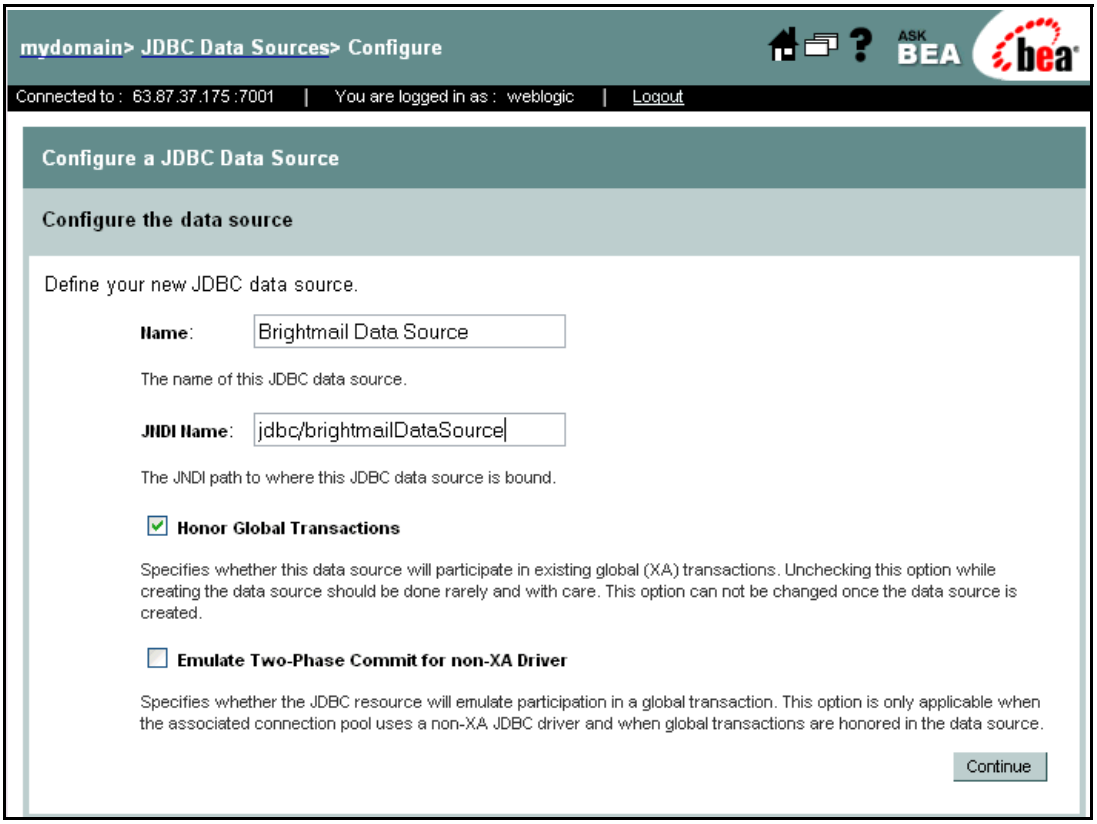
The page should appear similar to the picture above.

16 Click **Test Driver Configuration**.

17 Click **Create and deploy**.

Configuring a Data Source

1. Select the **JDBC Data Sources** page in the WebLogic management console by navigating to *your-domain*/**Services**/**JDBC**/**Data Sources**.
2. Click **Configure a new JDBC Data Source**.


mydomain> JDBC Data Sources> Configure
ASK BEA
Connected to : 63.87.37.175 :7001 | You are logged in as : weblogic | Logout
Configure a JDBC Data Source
Configure the data source
Define your new JDBC data source.
Name: Brightmail Data Source
The name of this JDBC data source.
JNDI Name: jdbc/brightmailDataSource
The JNDI path to where this JDBC data source is bound.
Honor Global Transactions
Specifies whether this data source will participate in existing global (XA) transactions. Unchecking this option while creating the data source should be done rarely and with care. This option can not be changed once the data source is created.
Emulate Two-Phase Commit for non-XA Driver
Specifies whether the JDBC resource will emulate participation in a global transaction. This option is only applicable when the associated connection pool uses a non-XA JDBC driver and when global transactions are honored in the data source.
Continue

3. In the **Name** box, type a name for your Data Source, for example `Brightmail Data Source`.
4. In the **JNDI Name** box, type `jdbc/brightmailDataSource`.

   The **Honor Global Transactions** and **Emulate Two-Phase Commit for non-XA Driver** check boxes can be left at the default setting. The page should appear similar to the picture above.
5. Click **Continue**.
6. Associate the data source with the connection pool you previously created.
7. Click **Continue**.

   The check boxes for the deployment targets can be left at the default setting.
8. Click **Create**.

Deploying the brightmail.war

1. Find the `brightmail.war` file, in the directory where you installed the Control Center. If the path to this file includes a space (for example, if it includes **Program Files**), move the `brightmail.war` file to a directory path that does not include any spaces.
2. Select the **Web Application Modules** hyperlink in the WebLogic Server console.
3. Click **Deploy a new Application Module…**
4. Navigate to the location of the `brightmail.war` file, either in the directory where you installed Control Center or in the directory you chose in Step 1.
5. Click **Target Module**.
6. In the **Name** field, type **`brightmail`**.
7. Click **Deploy**.

Testing the Control Center with the WebLogic Application Server

After following the steps in this section, ensure that the Brightmail Control Center and MySQL are communicating successfully by attempting to log into the Brightmail Control Center as described in the *Symantec Brightmail AntiSpam Administration Guide*.

Plug-Ins and Foldering

This section tells you how to install and configure the Symantec plug-in for Outlook and spam foldering agents for Microsoft Exchange and Lotus Domino users. It contains the following topics:

- Installing the Symantec Plug-in for Outlook
- Configuring Automatic Spam Foldering
- Enabling Automatic Spam Foldering

Installing the Symantec Plug-in for Outlook

The Symantec Plug-in for Outlook makes it easy for Outlook users to submit missed spam and false positives to Symantec. Depending on how you configure the plug-in, user submissions can also be automatically sent to a local system administrator. The Symantec Plug-in for Outlook also gives users the option to administer their own Blocked Senders and Allowed Senders Lists as well as specify languages in which they do or do not wish to receive email.

Usage Scenarios

You can use Symantec Plug-in for Outlook with the following other components of Symantec Brightmail AntiSpam:

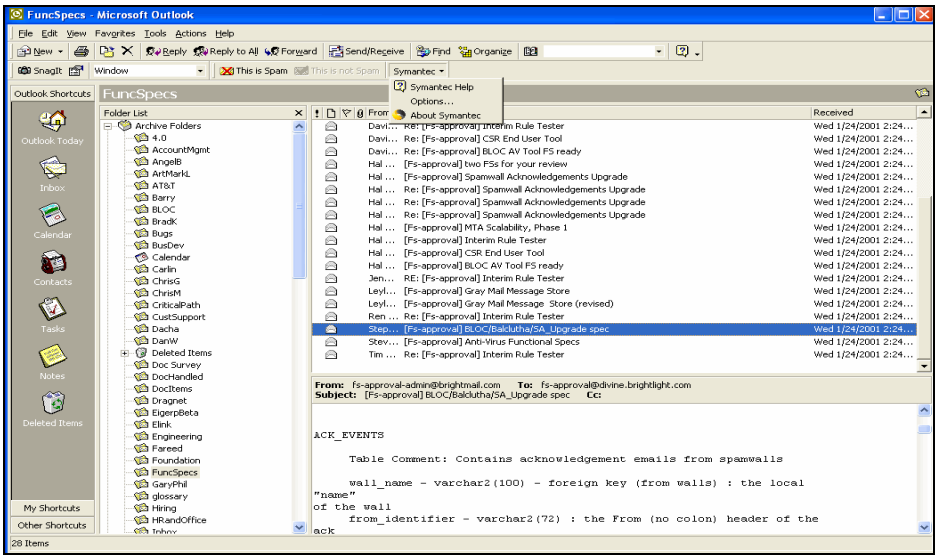
- Spam Folder Agent (or native MS Exchange foldering)
- Brightmail Quarantine
- Both Spam Folder Agent (or native MS Exchange foldering) and Brightmail Quarantine
- Neither Spam Folder Agent (or native MS Exchange foldering) nor Brightmail Quarantine

NOTE: *Refer to the Symantec Brightmail Anti-Spam Administration Guide for more information on Quarantine. To use native MS Exchange foldering, you must use Exchange 2003. See* "Configuring the Spam Folder Agent," on page 93 *for more information on the Spam Folder Agent and on native MS Exchange foldering.*

End User Experience

NOTE: *Documentation for end users is provided in the Symantec Plug-in for Outlook help system.*

After performing a simple installation process, users will have a new toolbar in their Outlook window:



- **This is Spam –** Users click this button to submit the message to the BLOC and move it from their Inbox to their Spam folder.
- **This is Not Spam –** Users click this button to submit the message to Symantec and move it from their Spam folder to their Inbox.
- **Empty Spam Folder –** Users click this button to empty their Spam folder (if configured)
- **Spam Quarantine –** Users click this button to launch Brightmail Quarantine in their default Web browser (if configured).
- **Symantec –** By choosing an item from this pull-down menu, users can get information on using the plug-in, view a report (if configured), and administer their personal Blocked Senders and Allowed Senders Lists.

Table 8. Symantec Menu Items

Menu Item	Description
Symantec Help	Launch a help page for the Symantec Plug-In for Outlook using your default Web browser.
Spam Report	View spam statistics (if configured).

Table 8. Symantec Menu Items (Continued)

Menu Item	Description
Options	Set plug-in properties and administer your private Blocked Senders and Allowed Senders Lists, specify languages in which you do or do not wish to receive email.
About Symantec	Get information on the current version of the software.

Software Requirements

The Symantec Plug-in for Outlook can be used with Outlook 2000, Outlook 2002, Outlook XP, and Outlook 2003, on Windows 98, Windows ME, Windows NT, Windows 2000, Windows XP, and Windows 2003.

NOTE: *If you are using Spam Folder Agent, the plug-in retrieves the name of the spam folder from the Spam Folder Agent Inbox Rule. Absent the Spam Folder Agent, the plug-in retrieves the* `SPAM_FOLDER` *value from the Windows registry. If there is no* `SPAM_FOLDER` *value in the Windows registry, it creates a Spam folder during installation.*

Administrator Setup Instructions

To set up the Symantec Plug-in for Outlook:

1. Do one of the following to navigate to the folder containing the Symantec Plug-in for Outlook software:

   If you are installing from a CD-ROM:

   a. Insert the Symantec Brightmail AntiSpam software distribution CD-ROM in your computer's CD-ROM drive.

   If the Installer runs automatically, click **Exit** to close the Installer.

   b. Open the **Windows\Plugin\Outlook** folder on the CD using Windows Explorer.

   If you are installing from a downloaded zip file:

   a. Unzip the zip file and extract all the contents to a folder.

   b. Open the **Plugin\Outlook** folder using Windows Explorer.

2. Copy all the files in the **Plugin\Outlook** folder to a network directory that is accessible to your users.

3. You can also modify the `setup.ini` file to configure system-wide settings. See the optional settings in Table 9, "Symantec Plug-in for Outlook Setup Variables," on page 90.

4 You can email your users a link to the `setup.exe` file in this directory, or use remote distribution software to install it on your users' computers. You can silently install by running `setup.exe` with the following switches: `/s /v"/qn"`

NOTE: *If you run* `setup.exe` *with the command* `/s /v"/qn"`*, the silent install option ignores changes made to* `setup.ini`*. To preserve your changes, add* `/qn` *to the end of the* `CmdLine` *attribute in* `setup.ini`*, and then run the silent install using:* `/s`*.*

NOTE: *Instruct users to close Outlook before running the installer by clicking* **File***, and then clicking* **Exit***. If they close Outlook in any other way, Outlook may continue to run in memory and return an error.*

To configure system-wide settings for the Symantec Plug-in for Outlook *(optional)***:**

1 Open the `setup.ini` file for editing. This file contains the initial settings for launching the Symantec Plug-in for Outlook installation package. All the settings you need to use can be set on the `CmdLine` attribute in the **[Startup]** section at the beginning of the `setup.ini` file. The settings will be added as values for the following Windows Registry key: `HKLM\Software\Brightmail\OutlookPlugin`

2 You can also change the settings in Table 9, "Symantec Plug-in for Outlook Setup Variables," on page 90.

Example:

```
CmdLine=SPAM_FOLDER="Junk"
ADMIN_FALSE_ADDRESS="admin-false@my.company.com"
```

Table 9. Symantec Plug-in for Outlook Setup Variables

Variable Name	Description
ADMIN_FALSE_ADDRESS	The email address of the administrator to copy with false positive submissions. The default for this is an empty string. If this value is empty, then the message will not be sent to the administrator.
ADMIN_JUNK_ADDRESS	The email address of the administrator to copy with missed spam submissions. The default for this is an empty string. If this value is empty, then the message will not be sent to the administrator.
ALLOW_CONTACTS	If set to **1** (the default) or any non-zero value, treat all entries of the Outlook Contacts folder as members of the Allowed Senders List. If set to **0**, do not treat any members of the Outlook Contacts folder as members of the Allowed Senders List.
AUTO_ADD_BLOCKED	When submitting a spam message to the BLOC, add the sender of the message to the Blocked Senders List. The default is **1**.

Table 9. Symantec Plug-in for Outlook Setup Variables (Continued)

Variable Name	Description
AUTO_ADD_ALLOWED	If set to **1** (the default) or any non-zero value, automatically generate the Allowed Senders list. If set to **0**, do not automatically generate the Allowed Senders list
AUTO_ALLOWED	If set to **1** (the default) or any non-zero value, automatically generate the Allowed Senders List. If set to **0**, do not automatically generate the Allowed Senders List.
CHECK_ALLOWED	If set to **1** (the default) or any non-zero value, move messages directly to the Spam folder. If a message sender is in the user's Allowed Senders List or (optionally) Outlook Contacts list, or if ANY of the message's recipients are in the user's Allowed Recipients List, the message is moved to the Inbox. Otherwise it stays in the Spam folder. If set to **0**, messages are delivered normally (to the Inbox).
CHECK_BLOCKED	If set to **1** (the default) or any non-zero value, move messages directly to the Spam folder. If a message sender is in the user's Allowed Senders List or (optionally) Outlook Contacts list, or if ANY of the message's recipients are in the user's Allowed Recipients List, the message is moved to the Inbox. Otherwise it stays in the Spam folder. If set to **0**, messages are delivered normally (to the Inbox).
DELETE_SPAM	If set to **1** or any non-zero value, spam messages will be deleted. If set to **0** (the default value), spam messages will be moved to the Spam folder.
DELETE_X_DAYS	Deletes messages in the Spam folder which are more than *x* days old. The default is **7**. Set this value to **0** to disable this feature.
DISPLAY_ARE_YOU_SURE_MSGS	Specifies whether the confirmation dialog is displayed after a message is submitted. If this variable is set to **1** (the default value) the confirmation message will be displayed. If this variable set to any other value or left empty, the message will not be displayed.
DISPLAY_CONFIRMATION_MSG	Specifies whether the confirmation dialog is displayed after a message is submitted. If this variable is set to **1** (the default value) the confirmation message will be displayed. If this variable set to any other value or left empty, the message will not be displayed.

Table 9. Symantec Plug-in for Outlook Setup Variables (Continued)

Variable Name	Description
EMPTY_SPAM_FOLDER	If set to **0** (the default), do not display the **Empty Spam** button. If set to **1** or any non-zero value, display the **Empty Spam** button. This button allows users to delete the contents of their Spam folders.
HIDE_NOT_SPAM	Specifies whether the **This is Not Spam** button is hidden. The default is **0** (displayed). Any non-zero value, including an empty value, will cause the button to be hidden.
HIDE_SPAM	Specifies whether the **This is Spam** button is hidden. The default is **0** (displayed). Any non-zero value, including an empty value, will cause the button to be hidden.
MANUAL_ALLOWED	If set to **1** (the default) or any non-zero value, allow users to add entries to the Allowed Senders and Allowed Recipients Lists. If set to **0**, do not allow users to add entries.
MANUAL_BLOCKED	If set to **1** (the default) or any non-zero value, allow users to add entries to the Allowed Senders and Allowed Recipients Lists. If set to **0**, do not allow users to add entries.
MARK_AS_READ	If set to **1** (the default) or any non-zero value, messages are marked as Read when moved to the Spam folder. If set to **0**, messages are not marked as Read when moved to the Spam folder.
MODIFY_OPTIONS	If set to **1** (the default) or any non-zero value, allow users to view/edit the **Submissions** and **Preferences** tabs. If set to **0**, do not allow users to view/edit the **Submissions** and **Preferences** tabs.
MULTI_CONFIRM_MSG	The confirmation message for multiple successful submissions. The default value for this string is: “Thank you for submitting messages to Symantec for review. We appreciate your help in improving our antispam service. This will be your only acknowledgement.”
SENDER_NOT_IN_ALLOWED	Specify the action to take if the message sender is not in the Allowed Senders List. • **Normal** – Move the message to the Inbox. • **Delete** – Delete the message. • **SpamFolder** – Move the message to the Spam folder. The default is **Normal**.

Table 9. Symantec Plug-in for Outlook Setup Variables (Continued)

Variable Name	Description
SINGLE_CONFIRM_MSG	The confirmation message for a single successful submission. The default value for this string is: “Thank you for submitting a message to Symantec for review. We appreciate your help in improving our antispam service. This will be your only acknowledgement.”
SPAM_FOLDER	The name of the Spam folder. The default is “**Spam**.”
SPAM_QUARANTINE_URL	If specified, this setting causes the **Spam Quarantine** button to appear in the toolbar. Clicking the button displays the Spam Quarantine login page in a Web browser. If unspecified (the default), the **Spam Quarantine** button does not appear in the toolbar.
REPORT_URL	If specified, this setting causes the **Spam Report** button to appear in the toolbar. Clicking the button displays the Spam Report application. If unspecified (the default), the **Spam Report** button does not appear in the toolbar.

3 Save your changes to the `setup.ini` file.

These settings will be used during each installation of the Symantec Plug-in for Outlook to modify the Windows Registry on each user’s computer.

Configuring Automatic Spam Foldering

You can route users’ spam into a special email folder so they can review it using the Spam Folder Agent or the Symantec Spam Folder Agent for Domino. To enable spam foldering after configuring it, see “Enabling Automatic Spam Foldering,” on page 105.

Configuring the Spam Folder Agent

See the *Symantec Brightmail AntiSpam Deployment Planning Guide* for detailed instructions for enabling spam foldering in Exchange 5.5 or Exchange 2000.

NOTE: *In certain configurations, Exchange 2003 will require no additional software to automatically route spam to a spam folder, but this must be enabled in the Brightmail Control Center. See* “Enabling Automatic Spam Foldering,” on page 105 *for more information. To use native foldering in Exchange 2003, you must deploy Exchange 2003 at the gateway and at the back end. In addition, users must enable the Junk Email Filter feature using Outlook 2003 or Outlook Web Access 2003. See the* Symantec Brightmail AntiSpam Deployment Planning Guide *for more details.*

To install the Spam Folder Agent (Exchange 5.5 or Exchange 2000):

1 Do one of the following to navigate to the **Setup.exe** file:

If you are installing from a CD-ROM:

a. Insert the Symantec software distribution CD-ROM in your computer's CD-ROM drive.

If the Installer does not run automatically, open the **Windows** folder on the CD using Windows Explorer and **Setup.exe**.

If you are installing from a downloaded zip file:

a. Unzip the zip file.

b. Double-click **Setup.exe**

2 Click **Next** to skip the introductory dialog box.

3 After reading the license agreement, click **I accept the terms of this license agreement**, and then click **Next**.

4 Choose a setup type, and then click **Next**.

Setup options include **Complete** and **Custom**. The **Complete** option installs all software in a predefined set of folders and files. The **Custom** option allows you to tailor installation options.

5 Under **Service Account**, specify an account to be used by the Spam Folder Agent. Type the Active Directory or NT Domain, as well as the user name and password.

For instructions on creating the service account for Exchange, see the *Symantec Brightmail AntiSpam Deployment Planning Guide.*

6 In the **Mailbox** field, specify the mailbox alias of a valid mailbox for the Spam Folder Agent to use.

To find this alias, click **Active Directory Users and Computers**, right-click User properties, and then click the **General** tab. The account specified in the last step must have Full Access to this mailbox.

7 In the **Spam folder name** field, specify the name of the folder in each end user's mailbox where spam will be foldered,

8 In the **Spam expiration** field, specify the period in days for which you want to retain spam messages. The default period is 30 days.

You may need to adjust this setting based on the volume of spam you receive at your organization.

9 Click **Next**.

10 Click **OK**.

NOTE: *If the installation process is unable to verify the existence of the spam folder because you have insufficient user rights, the following message is displayed. You can either continue without verification, or return to the* ***Configuration*** *dialog box and halt installation.*

Warning
You do not have access to verify these settings.
The "Act as part of the Operating System" user right is required to verify these settings.
Continue without verifying these settings?
Yes
No

11 Click **Install** to begin the installation process.

12 Click **Finish**.

The Installer configures the Spam Folder Agent as a Windows service that will run automatically. For information on how to change this default configuration, see "Enabling Automatic Spam Foldering," on page 105.

Configuring the Symantec Spam Folder Agent for Domino

To enable automatic foldering of spam for your Lotus Domino users, install the Symantec Spam Folder Agent for Domino on each Lotus Domino mail server.

Before you install the Symantec Spam Folder Agent for Domino, ensure your computer meets the following software and configuration requirements:

- Windows NT 4.0 (SP 3), Windows 2000 (SP 2), or Windows 2003.
- Lotus Notes Release 5.0.10 or later.

To install the Symantec Spam Folder Agent for Domino:

1 Do one of the following to navigate to the **Setup.exe** file:

If you are installing from a CD-ROM:

a. Insert the Symantec software distribution CD-ROM in your computer's CD-ROM drive.

If the Installer does not run automatically, open the **Windows** folder on the CD using Windows Explorer, and then double-click the **Setup.exe** icon.

If you are installing from a downloaded zip file:

a. Unzip the zip file.

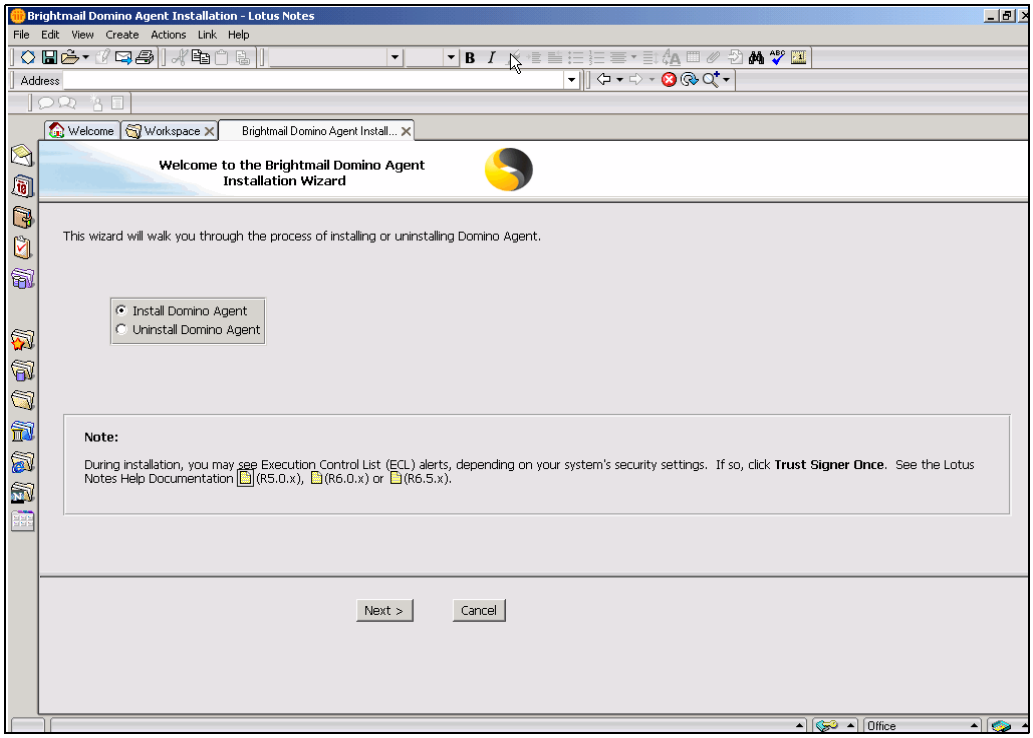
b. Double-click the **Setup.exe** icon.

2 Click **Brightmail Domino Agent**.

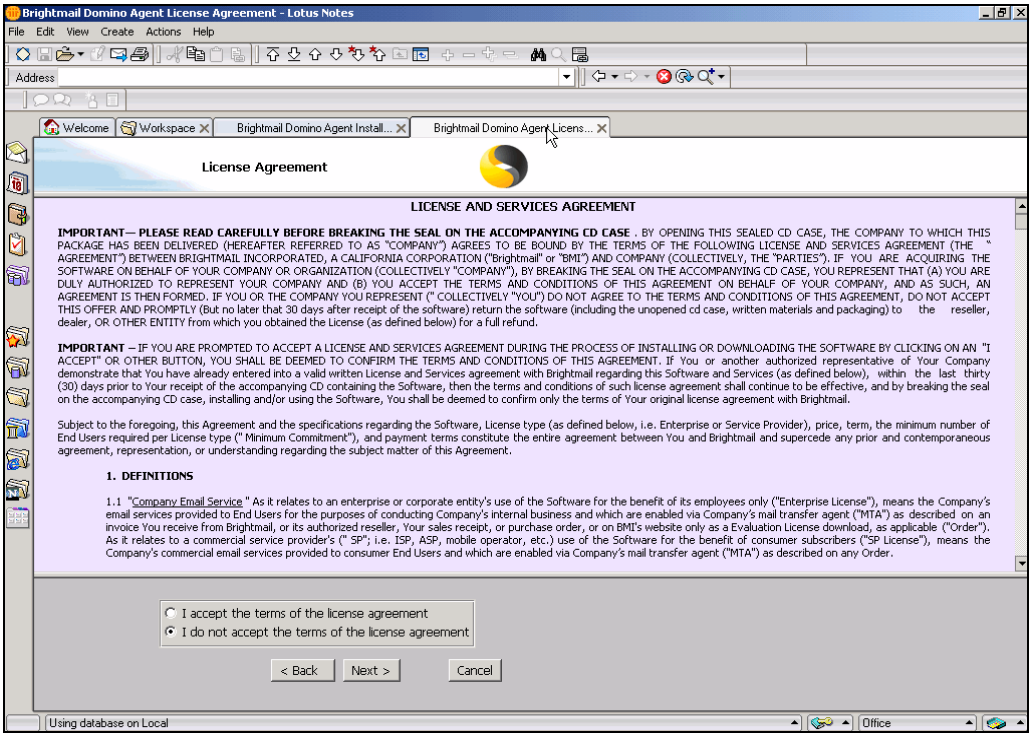
```
To continue installing Brightmail Domino Agent:

1) Start Lotus Notes.
2) Click File, then click Database, and then click Open.
3) In your Local directory, select Brightmail Domino Agent (BASAdmin.NSF).
4) Click Open.
```

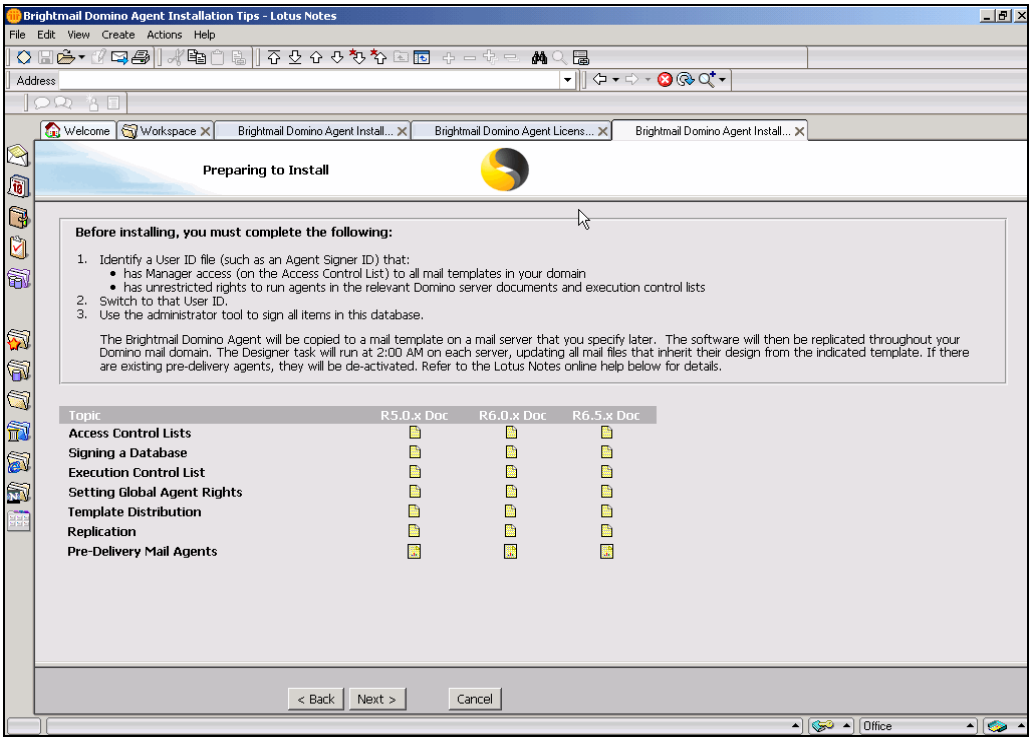
3 Follow the displayed instructions.


Brightmail Domino Agent Installation - Lotus Notes
File Edit View Create Actions Link Help
Address
Welcome
Workspace
Brightmail Domino Agent Install...
Welcome to the Brightmail Domino Agent Installation Wizard
This wizard will walk you through the process of installing or uninstalling Domino Agent.
Install Domino Agent
Uninstall Domino Agent
Note:
During installation, you may see Execution Control List (ECL) alerts, depending on your system's security settings. If so, click Trust Signer Once. See the Lotus Notes Help Documentation (R5.0.x), (R6.0.x) or (R6.5.x).
Next >
Cancel
Office

4 Click **Install Brightmail Domino Agent**, and then click **Next**.


Brightmail Domino Agent License Agreement - Lotus Notes
File Edit View Create Actions Help
Address
Welcome
Workspace
Brightmail Domino Agent Install...
Brightmail Domino Agent Licens...
License Agreement
LICENSE AND SERVICES AGREEMENT
IMPORTANT— PLEASE READ CAREFULLY BEFORE BREAKING THE SEAL ON THE ACCOMPANYING CD CASE . BY OPENING THIS SEALED CD CASE, THE COMPANY TO WHICH THIS PACKAGE HAS BEEN DELIVERED (HEREAFTER REFERRED TO AS "COMPANY") AGREES TO BE BOUND BY THE TERMS OF THE FOLLOWING LICENSE AND SERVICES AGREEMENT (THE " AGREEMENT") BETWEEN BRIGHTMAIL INCORPORATED, A CALIFORNIA CORPORATION ("Brightmail" or "BMI") AND COMPANY (COLLECTIVELY, THE "PARTIES"). IF YOU ARE ACQUIRING THE SOFTWARE ON BEHALF OF YOUR COMPANY OR ORGANIZATION (COLLECTIVELY "COMPANY"), BY BREAKING THE SEAL ON THE ACCOMPANYING CD CASE, YOU REPRESENT THAT (A) YOU ARE DULY AUTHORIZED TO REPRESENT YOUR COMPANY AND (B) YOU ACCEPT THE TERMS AND CONDITIONS OF THIS AGREEMENT ON BEHALF OF YOUR COMPANY, AND AS SUCH, AN AGREEMENT IS THEN FORMED. IF YOU OR THE COMPANY YOU REPRESENT (" COLLECTIVELY "YOU") DO NOT AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT, DO NOT ACCEPT THIS OFFER AND PROMPTLY (But no later that 30 days after receipt of the software) return the software (including the unopened cd case, written materials and packaging) to the reseller, dealer, OR OTHER ENTITY from which you obtained the License (as defined below) for a full refund.
IMPORTANT – IF YOU ARE PROMPTED TO ACCEPT A LICENSE AND SERVICES AGREEMENT DURING THE PROCESS OF INSTALLING OR DOWNLOADING THE SOFTWARE BY CLICKING ON AN "I ACCEPT" OR OTHER BUTTON, YOU SHALL BE DEEMED TO CONFIRM THE TERMS AND CONDITIONS OF THIS AGREEMENT. If You or another authorized representative of Your Company demonstrate that You have already entered into a valid written License and Services agreement with Brightmail regarding this Software and Services (as defined below), within the last thirty (30) days prior to Your receipt of the accompanying CD containing the Software, then the terms and conditions of such license agreement shall continue to be effective, and by breaking the seal on the accompanying CD case, installing and/or using the Software, You shall be deemed to confirm only the terms of Your original license agreement with Brightmail.
Subject to the foregoing, this Agreement and the specifications regarding the Software, License type (as defined below, i.e. Enterprise or Service Provider), price, term, the minimum number of End Users required per License type (" Minimum Commitment"), and payment terms constitute the entire agreement between You and Brightmail and supercede any prior and contemporaneous agreement, representation, or understanding regarding the subject matter of this Agreement.
1. DEFINITIONS
1.1 "Company Email Service " As it relates to an enterprise or corporate entity's use of the Software for the benefit of its employees only ("Enterprise License"), means the Company's email services provided to End Users for the purposes of conducting Company's internal business and which are enabled via Company's mail transfer agent ("MTA") as described on an invoice You receive from Brightmail, or its authorized reseller, Your sales receipt, or purchase order, or on BMI's website only as a Evaluation License download, as applicable ("Order"). As it relates to a commercial service provider's (" SP"; i.e. ISP, ASP, mobile operator, etc.) use of the Software for the benefit of consumer subscribers ("SP License"), means the Company's commercial email services provided to consumer End Users and which are enabled via Company's mail transfer agent ("MTA") as described on any Order.
I accept the terms of the license agreement
I do not accept the terms of the license agreement
< Back
Next >
Cancel
Using database on Local
Office

5 After reading the license agreement, click **I accept the terms of the license agreement**, and then click **Next.**


Brightmail Domino Agent Installation Tips - Lotus Notes
File Edit View Create Actions Help
Address
Welcome
Workspace
Brightmail Domino Agent Install...
Brightmail Domino Agent Licens...
Brightmail Domino Agent Install...
Preparing to Install
Before installing, you must complete the following:
1. Identify a User ID file (such as an Agent Signer ID) that:
• has Manager access (on the Access Control List) to all mail templates in your domain
• has unrestricted rights to run agents in the relevant Domino server documents and execution control lists
2. Switch to that User ID.
3. Use the administrator tool to sign all items in this database.
The Brightmail Domino Agent will be copied to a mail template on a mail server that you specify later. The software will then be replicated throughout your Domino mail domain. The Designer task will run at 2:00 AM on each server, updating all mail files that inherit their design from the indicated template. If there are existing pre-delivery agents, they will be de-activated. Refer to the Lotus Notes online help below for details.
Topic
R5.0.x Doc
R6.0.x Doc
R6.5.x Doc
Access Control Lists
Signing a Database
Execution Control List
Setting Global Agent Rights
Template Distribution
Replication
Pre-Delivery Mail Agents
< Back
Next >
Cancel
Office

6 Complete all prerequisite steps if you haven't already done so.

Caution

On each server in your environment running Lotus Notes Release 5, you must add the following variable to the `Notes.INI` *file:*

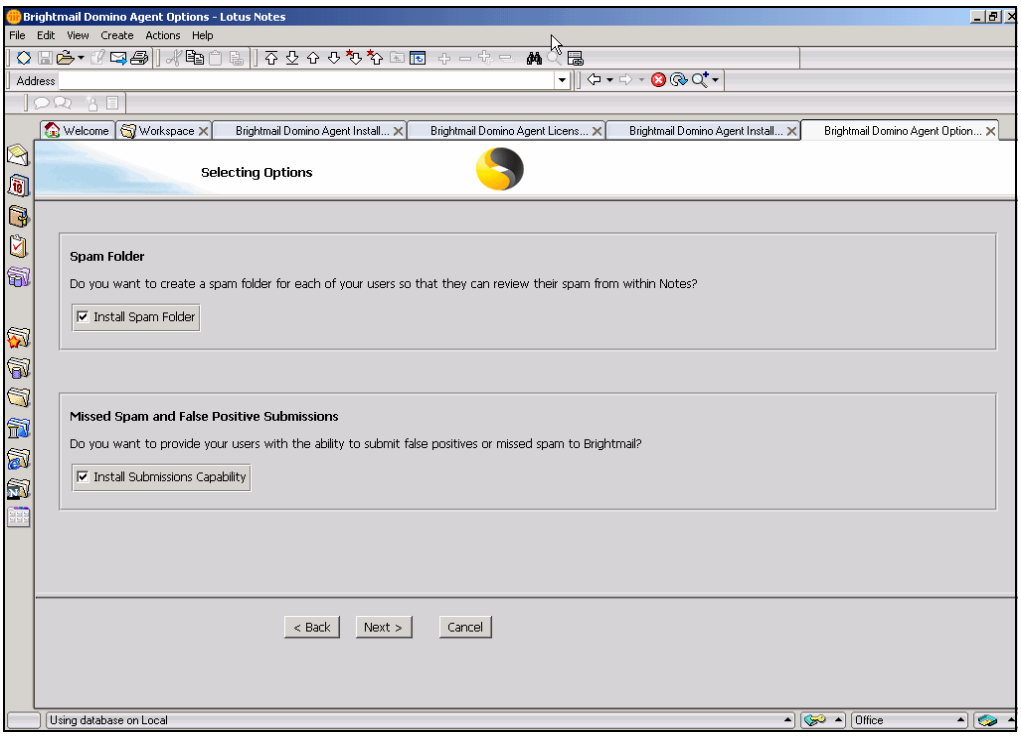
`Amgr_DisableMailLookup=1`

`Notes.INI` *is usually found in the server's root* `Notes` *folder.*

You should then restart each server running Release 5. (This setting is not required for servers running Release 6.) For more information, search for document #1099178 on the Lotus support page:

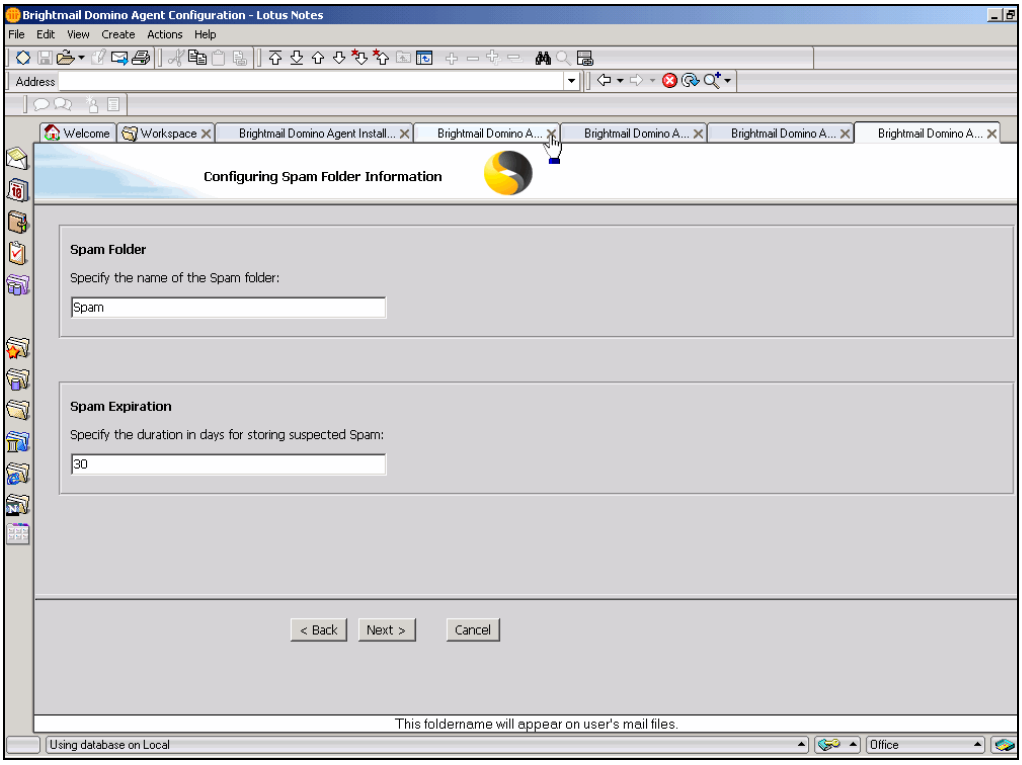
`http://www-3.ibm.com/software/lotus/support/`

7 Click **Next**.


Brightmail Domino Agent Options - Lotus Notes
File Edit View Create Actions Help
Address
Welcome
Workspace
Brightmail Domino Agent Install...
Brightmail Domino Agent Licens...
Brightmail Domino Agent Install...
Brightmail Domino Agent Option...
Selecting Options
Spam Folder
Do you want to create a spam folder for each of your users so that they can review their spam from within Notes?
Install Spam Folder
Missed Spam and False Positive Submissions
Do you want to provide your users with the ability to submit false positives or missed spam to Brightmail?
Install Submissions Capability
< Back
Next >
Cancel
Using database on Local
Office

8 Select the option(s) you wish to configure.

9 Click **Next**.

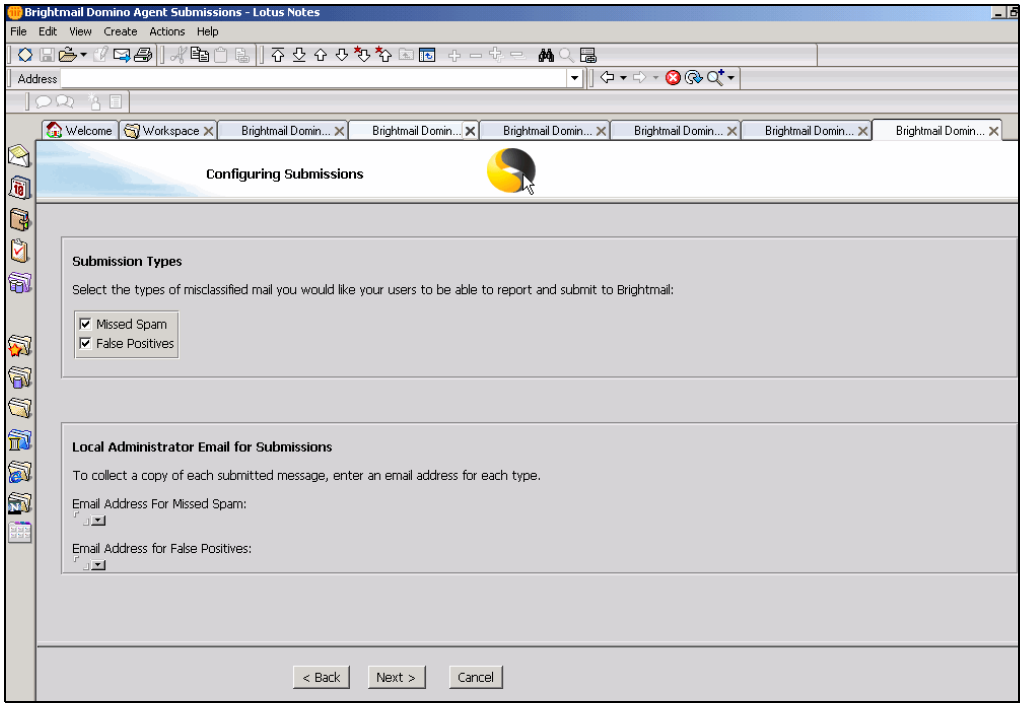


NOTE: *This screen is displayed only if you chose to configure spam foldering.*

10 Under **Spam Folder**, specify the name of the folder in each end user's mailbox where spam will be sidelined, and then click **Next**. The default is **Spam**.

11 Specify a spam expiration between 1 and 365 days. Messages will be automatically deleted from the Spam folder after the specified number of days. The default is **30** days.

12 Click **Next**.

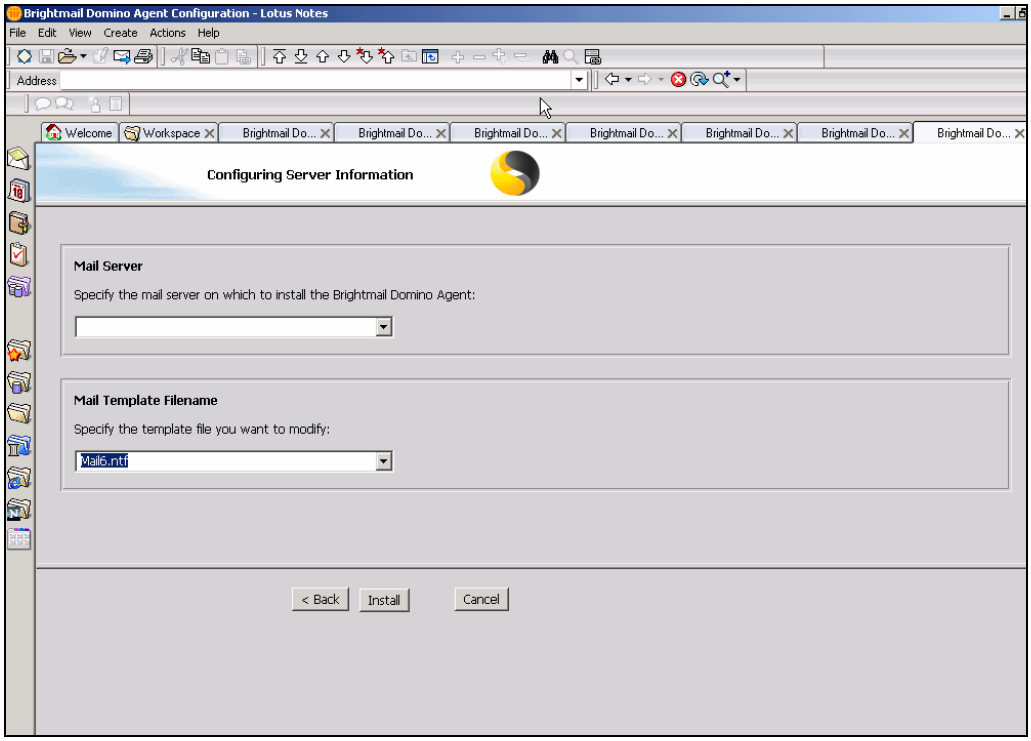

Brightmail Domino Agent Submissions - Lotus Notes
File Edit View Create Actions Help
Address
Welcome
Workspace
Brightmail Domin...
Configuring Submissions
Submission Types
Select the types of misclassified mail you would like your users to be able to report and submit to Brightmail:
Missed Spam
False Positives
Local Administrator Email for Submissions
To collect a copy of each submitted message, enter an email address for each type.
Email Address For Missed Spam:
Email Address for False Positives:
< Back
Next >
Cancel

NOTE: *This screen is displayed only if you chose to configure missed spam and false positive submissions.*

13 Under **Submission Types**, select **Missed Spam**, **False Positives**, or both.

14 Under **Local Administrator Email for Submissions**, either select an email address from the drop down list adjacent the submission type(s) you wish to configure or type the address.

15 Click **Next**.



16 Specify a mail server.

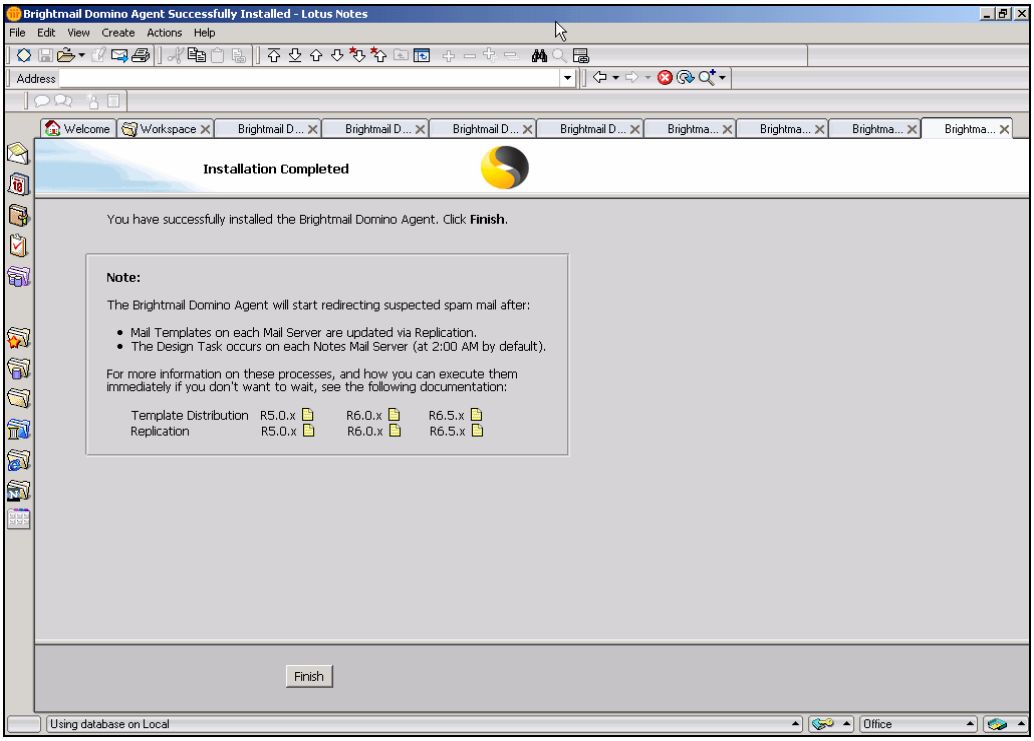
NOTE: *If your mail template files are replicas (as they are when shipped), you need only install the Symantec Spam Folder Agent for Domino on one server.*

17 Specify a mail template filename.

NOTE: *You must repeat this process for each mail template used at your site.*

18 Click **Install**.

NOTE: *To reconfigure the Symantec Spam Folder Agent for Domino, you should first uninstall it, then reinstall it.*


Brightmail Domino Agent Successfully Installed - Lotus Notes
File Edit View Create Actions Help
Address
Welcome
Workspace
Installation Completed
You have successfully installed the Brightmail Domino Agent. Click Finish.
Note:
The Brightmail Domino Agent will start redirecting suspected spam mail after:
Mail Templates on each Mail Server are updated via Replication.
The Design Task occurs on each Notes Mail Server (at 2:00 AM by default).
For more information on these processes, and how you can execute them immediately if you don't want to wait, see the following documentation:
Template Distribution R5.0.x R6.0.x R6.5.x
Replication R5.0.x R6.0.x R6.5.x
Finish
Using database on Local
Office

19 Click **Finish**.

The mail server on which you install the Symantec Spam Folder Agent for Domino distributes changes to all other mail servers in your environment as part of the Design task, which runs overnight.

The Symantec Spam Folder Agent for Domino will not be visible on each user's mail file until:

- Replication distributes the change to the template on the user's home mail server.
- The nightly Design process runs on the user's home mail server.
- The user reopens his or her mail file after installation.

  This only applies if the user's mail file was open when its design was refreshed. The Symantec Spam Folder Agent for Domino will take effect when the design is refreshed, though the folder will not be visible.

See the Lotus Notes online help for information on forcing changes immediately.

Distributing End-User Help

The Symantec Spam Folder Agent for Domino installer includes an MS Word file (`BMIEndUser.doc`) detailing the submission process.

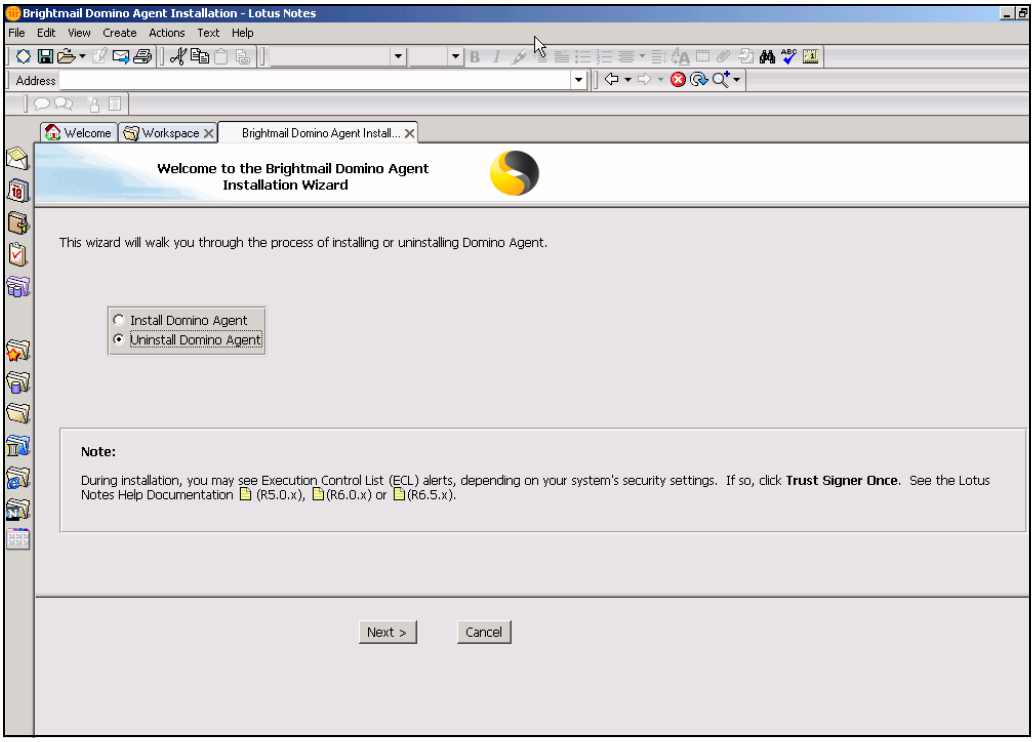
You can distribute this information to your users in two ways:

- Import `BMIEndUser.doc` or email it as an attachment to all end users.

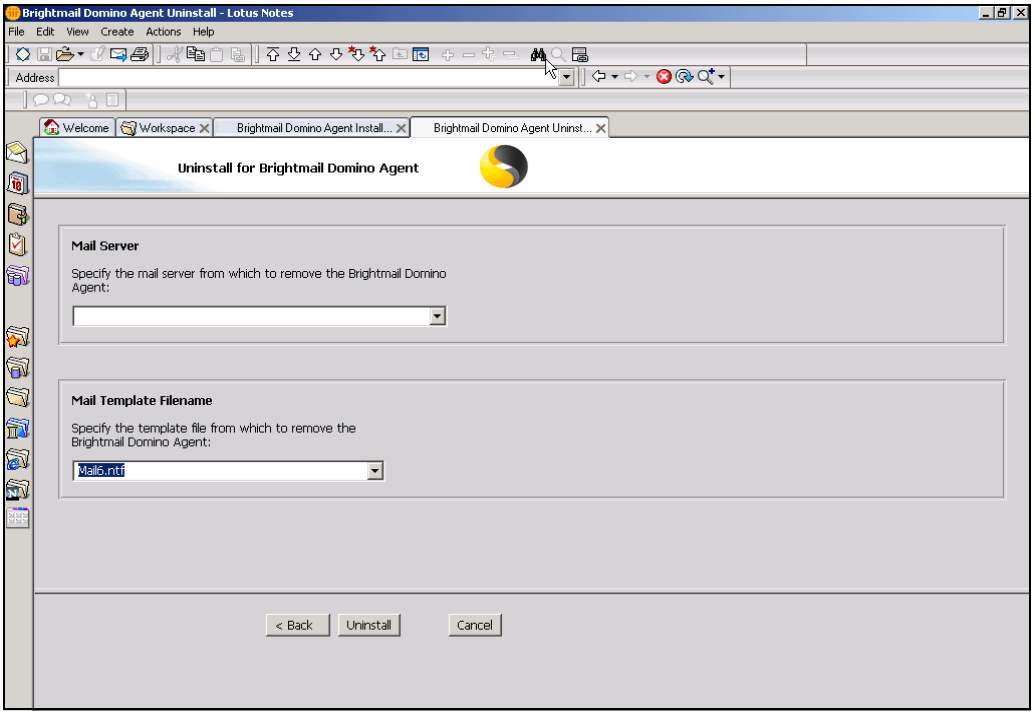
- Add the information in `BMIEndUser.doc` to the **Help Using** document of the mail template so that users have it available at all times.

To uninstall the Symantec Spam Folder Agent for Domino:

1 Click **Brightmail Domino Agent** in the **Installer** screen.

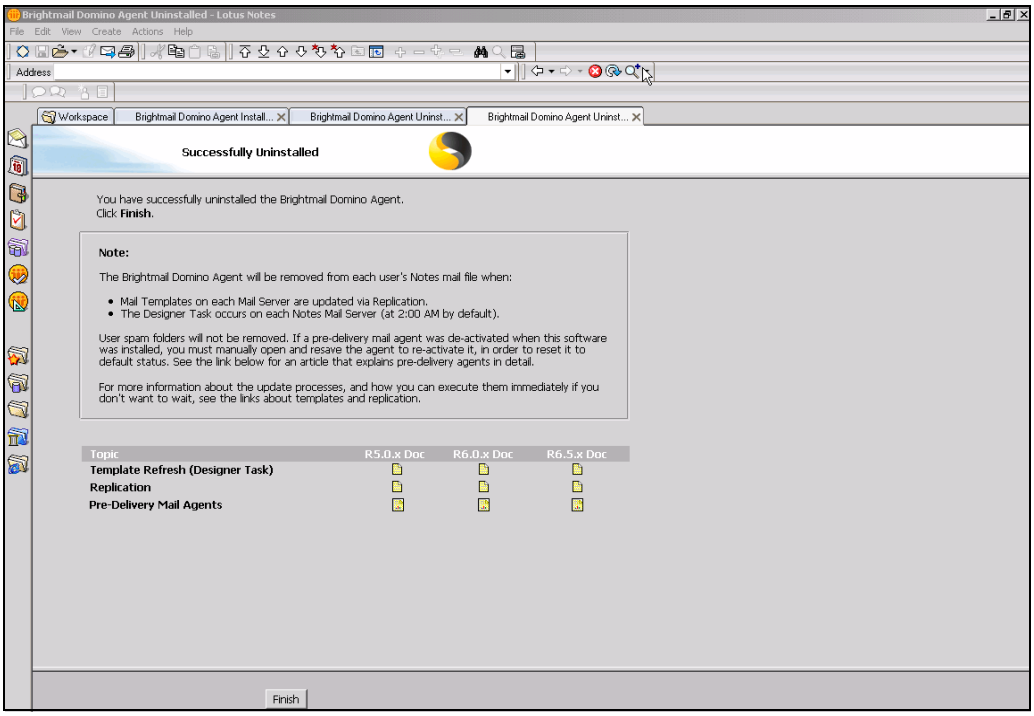

Brightmail Domino Agent Installation - Lotus Notes
File Edit View Create Actions Text Help
Address
Welcome
Workspace
Brightmail Domino Agent Install...
Welcome to the Brightmail Domino Agent Installation Wizard
This wizard will walk you through the process of installing or uninstalling Domino Agent.
Install Domino Agent
Uninstall Domino Agent
Note:
During installation, you may see Execution Control List (ECL) alerts, depending on your system's security settings. If so, click Trust Signer Once. See the Lotus Notes Help Documentation (R5.0.x), (R6.0.x) or (R6.5.x).
Next >
Cancel

2 Click **Uninstall Brightmail Domino Agent**, and then click **Next**.



3 Click **Uninstall**.

NOTE: *If your mail template files are replicas (as they are when shipped), you need only uninstall once.*


Brightmail Domino Agent Uninstalled - Lotus Notes
File Edit View Create Actions Help
Address
Workspace
Brightmail Domino Agent Install...
Brightmail Domino Agent Uninst...
Brightmail Domino Agent Uninst...
Successfully Uninstalled
You have successfully uninstalled the Brightmail Domino Agent.
Click Finish.
Note:
The Brightmail Domino Agent will be removed from each user's Notes mail file when:
Mail Templates on each Mail Server are updated via Replication.
The Designer Task occurs on each Notes Mail Server (at 2:00 AM by default).
User spam folders will not be removed. If a pre-delivery mail agent was de-activated when this software was installed, you must manually open and resave the agent to re-activate it, in order to reset it to default status. See the link below for an article that explains pre-delivery agents in detail.
For more information about the update processes, and how you can execute them immediately if you don't want to wait, see the links about templates and replication.
Topic
R5.0.x Doc
R6.0.x Doc
R6.5.x Doc
Template Refresh (Designer Task)
Replication
Pre-Delivery Mail Agents
Finish

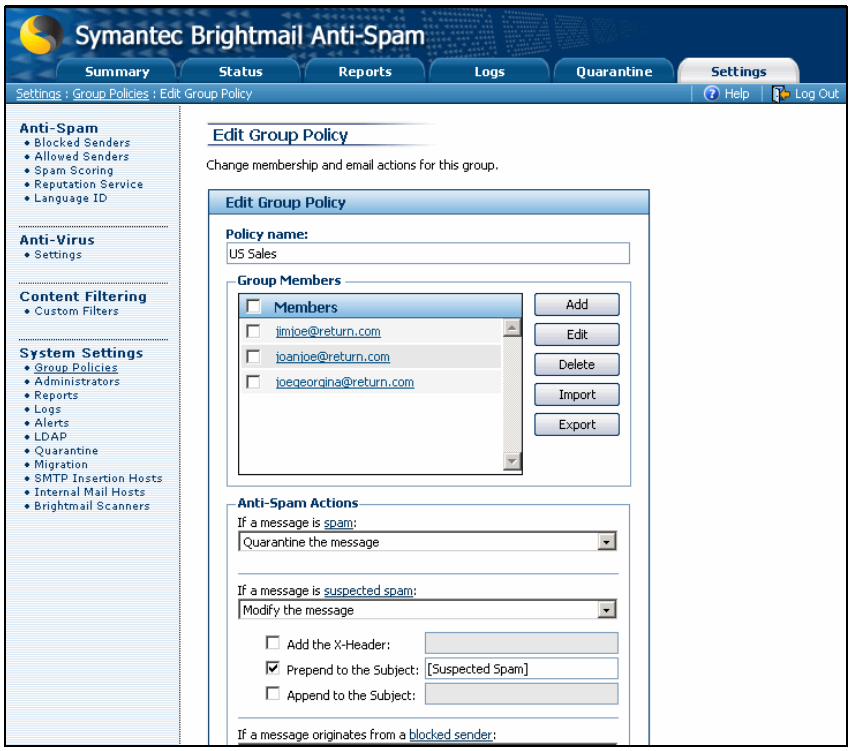
4 Click **Finish**.

Enabling Automatic Spam Foldering

Follow these steps to enable automatic spam foldering for Exchange 5.5 or 2000, Exchange 2003, or Lotus Domino.

1 In the Brightmail Control Center, click on the **Settings** tab. Choose **Group Policies** in the menu in the left pane. If you have more than one group policy, repeat the steps below for each group that will use spam foldering.

2 Click on the group policy name to view the **Edit Group Policy** screen. On this screen you can choose message handling options for each category of messages received by the members of this group policy.



3 For each category of messages that you want to go to user spam folders, click on the pull-down menu and choose **Deliver the message to the recipient's Spam folder**.

4 When you have made all of your choices, click **Save**.

Appendix A: Symantec Brightmail AntiSpam Files

This Appendix provides detailed information on the directory structure, file locations, and permissions and ownership for Symantec Brightmail AntiSpam software. These defaults are listed to help you configure your implementation.

The following lists display the default locations and settings for permissions andownership for Symantec software files, by directory. An asterisk (`*`) designates an executable file.

In all of the following, the `jre` directory, which is installed by InstallAnywhere and which Symantec does not control, is not listed. Directory listings assume "pwd" is the installation directory.

NOTE: *In the following lists, the .1 suffix of some files and directories is replaced by a timestamp when Symantec Brightmail AntiSpam is executing. Both the directory name and contents can change during program execution.*

This appendix includes the following sections:

- Brightmail Scanner on UNIX
  - Brightmail Scanner, Complete (Brightmail Server, Brightmail Client)
  - Brightmail Scanner Installation with Brightmail Server Only
  - Brightmail Scanner Installation with Brightmail Client Only
- Brightmail Scanner on Windows
  - Brightmail Scanner, Complete (Brightmail Server, Brightmail Client)
  - Brightmail Scanner Installation with Brightmail Server Only
  - Brightmail Scanner Installation with Brightmail Client Only
- Brightmail Control Center on All Platforms

Brightmail Scanner on UNIX

Brightmail Scanner, Complete (Brightmail Server, Brightmail Client)

```
-rw-rw-r--    1 root     root  Brightmail_Anti-Spam_InstallLog.log
-r--r--r--    1 mailwall bmi   EULA
-rw-r--r--    1 mailwall bmi   LEGAL.NOTICES.txt
drwxrwxr-x    2 root     root  UninstallerData/
drwxr-x---    2 mailwall bmi   bin/
drwxrwx---    2 mailwall bmi   bm_ruleset.2.avsym.1/
drwxrwx---    2 mailwall bmi   bm_ruleset.2.permit_rules.1/
drwxrwx---    2 mailwall bmi   bm_ruleset.2.spamhunter_rules.1/
drwxrwx---    2 mailwall bmi   bm_ruleset.2.spamsig_rules.1/
drwxr-xr-x    2 mailwall bmi   docs/
drwxr-xr-x    5 mailwall bmi   etc/
-rw-rw----    1 mailwall bmi   hashes
drwxr-x---    5 mailwall bmi   jobs/
drwxr-x---    2 mailwall bmi   lib/
drwxr-x---    2 mailwall bmi   sbin/
-rw-rw-r--    1 mailwall bmi   sieve_script.txt
drwxr-x---    2 mailwall bmi   stats/
```

./UninstallerData:

```
-rw-rw-r--    1 root     root  InstallScript.iap_xml
-r-xr-x---    1 root     root  Uninstall*
-rwxrwxr-x    1 root     root  Uninstall.lax*
-rw-rw-r--    1 root     root  installvariables.properties
-rwxr-xr-x    1 root     root  remove.bssas.cron.sh*
-rwxrwxr-x    1 root     root  remove.bssav.cron.sh*
-rw-rw-r--    1 root     root  uninstaller.jar
```

./bin:

```
-r-xr-x---    1 mailwall bmi  av_cleaner*
-rwxr-x---    1 mailwall bmi  bmifilter*
-r-xr-x---    1 mailwall bmi  bmserver*
-r-xr-x---    1 mailwall bmi  conduit*
-r-xr-x---    1 mailwall bmi  harvester*
-r-xr-x---    1 mailwall bmi  kicker*
```

./bm_ruleset.2.avsym.1:

```
-rw-rw----    1 mailwall bmi  catalog.dat
-rw-rw----    1 mailwall bmi  navensol.so
-rw-rw----    1 mailwall bmi  navexsol.so
-rw-rw----    1 mailwall bmi  navupsol.dis
-rw-rw----    1 mailwall bmi  ncsacert.txt
-rw-rw----    1 mailwall bmi  scrauth.dat
-rw-rw----    1 mailwall bmi  technote.txt
-rw-rw----    1 mailwall bmi  tinf.dat
-rw-rw----    1 mailwall bmi  tinfidx.dat
-rw-rw----    1 mailwall bmi  tinfl.dat
-rw-rw----    1 mailwall bmi  tscan1.dat
-rw-rw----    1 mailwall bmi  tscan1hd.dat
-rw-rw----    1 mailwall bmi  update.txt
-rw-rw----    1 mailwall bmi  virscan.inf
-rw-rw----    1 mailwall bmi  virscan1.dat
-rw-rw----    1 mailwall bmi  virscan2.dat
-rw-rw----    1 mailwall bmi  virscan3.dat
-rw-rw----    1 mailwall bmi  virscan4.dat
-rw-rw----    1 mailwall bmi  virscan5.dat
-rw-rw----    1 mailwall bmi  virscan6.dat
-rw-rw----    1 mailwall bmi  virscan7.dat
-rw-rw----    1 mailwall bmi  virscan8.dat
-rw-rw----    1 mailwall bmi  virscan9.dat
-rw-rw----    1 mailwall bmi  whatsnew.txt
-rw-rw----    1 mailwall bmi  zdone.dat
```

./bm_ruleset.2.permit_rules.1:

```
-rw-rw----    1 mailwall bmi  permit_rules
```

./bm_ruleset.2.spamhunter_rules.1:

```
-rw-rw----    1 mailwall bmi  rules
```

./bm_ruleset.2.spamsig_rules.1:

```
-rw-rw----    1 mailwall bmi  spamsigs
```

./docs:

```
-rw-r--r--    1 mailwall bmi  documentation.html
```

./etc:

```
-r--r-----    1 mailwall bmi  AdvisoryStore.dtd
-rw-rw----    1 mailwall bmi  Notification.xml
-r--r--r--    1 mailwall bmi  agent.cert
-rw-rw-r--    1 mailwall bmi  agentconfig.xml
-r--r--r--    1 mailwall bmi  agent.key
drwxrwxr-x    2 mailwall bmi  bm_ruleset.2.avsym.1.sample/
-rw-rw-r--    1 mailwall bmi  bmiconfig.xml
-rwxrwxr-x    1 mailwall bmi  brightmail-env*
-r--r-----    1 mailwall bmi  hashes.sample
-rwx------    1 mailwall bmi  patchinstall*
-r--r-----    1 mailwall bmi  permit_rules.sample
-r-xr-x---    1 mailwall bmi  process-cleanup*
-r--r-----    1 mailwall bmi  rules.sample
-rw-rw-r--    1 mailwall bmi  runner.cfg
-rw-r-----    1 mailwall bmi  sieve_adult.sample
-rw-r-----    1 mailwall bmi  sieve_script.sample
-r--r-----    1 mailwall bmi  spamsigs.sample
drwxrwxr-x    2 mailwall bmi  tests/
-r--r--r--    1 mailwall bmi  trusted.cert
-rw-rw-r--    1 mailwall bmi  allowedblockedlist.txt
```

./etc/bm_ruleset.2.avsym.1.sample:

```
-rw-rw----    1 mailwall bmi  catalog.dat
-rw-rw----    1 mailwall bmi  navensol.so (on linux, this is navenlin.so)
-rw-rw----    1 mailwall bmi  navexsol.so (on linux, this is navexlin.so)
-rw-rw----    1 mailwall bmi  navupsol.dis (on linux, this is navuplin.so)
-rw-rw----    1 mailwall bmi  ncsacert.txt
-rw-rw----    1 mailwall bmi  scrauth.dat
-rw-rw----    1 mailwall bmi  technote.txt
-rw-rw----    1 mailwall bmi  tinf.dat
-rw-rw----    1 mailwall bmi  tinfidx.dat
-rw-rw----    1 mailwall bmi  tinfl.dat
-rw-rw----    1 mailwall bmi  tscan1.dat
-rw-rw----    1 mailwall bmi  tscan1hd.dat
-rw-rw----    1 mailwall bmi  update.txt
-rw-rw----    1 mailwall bmi  virscan.inf
-rw-rw----    1 mailwall bmi  virscan1.dat
```

```
-rw-rw----    1 mailwall bmi  virscan2.dat
-rw-rw----    1 mailwall bmi  virscan3.dat
-rw-rw----    1 mailwall bmi  virscan4.dat
-rw-rw----    1 mailwall bmi  virscan5.dat
-rw-rw----    1 mailwall bmi  virscan6.dat
-rw-rw----    1 mailwall bmi  virscan7.dat
-rw-rw----    1 mailwall bmi  virscan8.dat
-rw-rw----    1 mailwall bmi  virscan9.dat
-rw-rw----    1 mailwall bmi  whatsnew.txt
-rw-rw----    1 mailwall bmi  zdone.dat
```

./etc/tests:

```
drwxrwxr-x    2 mailwall bmi  lang_id/
-rw-r-----    1 mailwall bmi  rules.msg
-rw-r-----    1 mailwall bmi  sieve.adult.msg
-rw-r-----    1 mailwall bmi  sieve.sideline.msg
-rw-r-----    1 mailwall bmi  spamsig.msg
```

./etc/tests/lang_id:

```
-rw-r-----    1 mailwall bmi  de.eml
-rw-r-----    1 mailwall bmi  es.eml
-rw-r-----    1 mailwall bmi  fr.eml
-rw-r-----    1 mailwall bmi  it.eml
-rw-r-----    1 mailwall bmi  ja.eml
-rw-r-----    1 mailwall bmi  ko.eml
-rw-r-----    1 mailwall bmi  nl.eml
-rw-r-----    1 mailwall bmi  pt.eml
-rw-r-----    1 mailwall bmi  ru.eml
-rw-r-----    1 mailwall bmi  zh.eml
```

./jobs:

```
drwxr-x---    2 mailwall bmi  bmagent/
drwxrwx---    2 mailwall bmi  bmifilter/
drwxr-x---    2 mailwall bmi  bmserver/
drwxr-x---    2 mailwall bmi  conduit/
drwxr-x---    2 mailwall bmi  harvester/
```

./jobs/bmagent:

./jobs/bmifilter:

```
-rw-r-----    2 mailwall bmi  bmifilter.stop
```

./jobs/bmserver:

```
-rw-r-----    2 mailwall bmi  bmserver.stop
```

./jobs/conduit:

```
-rw-r-----    2 mailwall bmi  conduit.stop
```

./jobs/harvester:

```
-rw-r-----    2 mailwall bmi  harvester.stop
```

./lib:

```
-rwxr-xr-x    1 mailwall bmi  libACE.so.5.4.0*
lrwxrwxrwx    1 root     root libACE.so -> ./libACE.so.5.4.0*
-rwxr-xr-x    1 mailwall bmi  libACE_SSL.so.5.4.0*
lrwxrwxrwx    1 root     root libACE_SSL.so -> ./libACE_SSL.so.5.4.0*
-r--r-----    1 mailwall bmi  libantivirus.so
-r--r-----    1 mailwall bmi  libbh.so
-r-xr-xr-x    1 mailwall bmi  libbmiclient.so.1*
-r-xr-xr-x    1 mailwall bmi  libbmishareddata.so*
-r-xr-x---    1 mailwall bmi  libbmiutil.so.1*
lrwxrwxrwx    1 root     root libicudata.so -> ./libicudata.so.28*
-rwxr-xr-x    1 mailwall bmi  libicudata.so.28*
lrwxrwxrwx    1 root     root libicui18n.so -> ./libicui18n.so.28*
-rwxr-xr-x    1 mailwall bmi  libicui18n.so.28*
lrwxrwxrwx    1 root     root libicuuc.so -> ./libicuuc.so.28*
-rwxr-xr-x    1 mailwall bmi  libicuuc.so.28*
-r--r-----    1 mailwall bmi  liblanguageid.so
-r--r-----    1 mailwall bmi  libpermit.so
-r--r-----    1 mailwall bmi  libregexfilter.so
-r--r-----    1 mailwall bmi  libreinsert.so
-r--r-----    1 mailwall bmi  libsieve.so
-r--r-----    1 mailwall bmi  libspamhunter.so
-r--r-----    1 mailwall bmi  libspamsig.so
-rwxr-xr-x    1 mailwall bmi  libstlport_gcc.so*
-rwxr-xr-x    1 mailwall bmi  libxml2.so.2*
lrwxrwxrwx    1 root     root libxml2.so -> ./libxml2.so.2*
```

./sbin:

```
-r-xr-x---    1 mailwall bmi  bmagent*
-r-xr-x---    1 mailwall bmi  controller.sh*
-r-xr-x---    1 mailwall bmi  inspector*
-r-xr-x---    1 mailwall bmi  register*
-r-xr-x---    1 mailwall bmi  register.sh*
-r-xr-x---    1 mailwall bmi  runcleaner.sh*
-r-xr-x---    1 mailwall bmi  runner*
```

./stats:

Brightmail Scanner Installation with Brightmail Server Only

```
-rw-rw-r--    1 root     root Brightmail_Anti-Spam_InstallLog.log
-r--r--r--    1 mailwall bmi  EULA
-rw-r--r--    1 mailwall bmi  LEGAL.NOTICES.txt
drwxrwxr-x    2 root     root UninstallerData/
drwxr-x---    2 mailwall bmi  bin/
drwxrwx---    2 mailwall bmi  bm_ruleset.2.avsym.1/
drwxrwx---    2 mailwall bmi  bm_ruleset.2.permit_rules.1/
drwxrwx---    2 mailwall bmi  bm_ruleset.2.spamhunter_rules.1/
drwxrwx---    2 mailwall bmi  bm_ruleset.2.spamsig_rules.1/
drwxr-xr-x    2 mailwall bmi  docs/
drwxr-xr-x    5 mailwall bmi  etc/
-rw-rw----    1 mailwall bmi  hashes
drwxr-x---    4 mailwall bmi  jobs/
drwxr-x---    2 mailwall bmi  lib/
drwxrwxr-x    2 mailwall bmi  logs/
drwxr-x---    2 mailwall bmi  sbin/
-rw-rw-r--    1 mailwall bmi  sieve_script.txt
drwxr-x---    2 mailwall bmi  stats/
```

./UninstallerData:

```
-rw-rw-r--    1 root     root InstallScript.iap_xml
-r-xr-x---    1 root     root Uninstall*
-rwxrwxr-x    1 root     root Uninstall.lax*
-rw-rw-r--    1 root     root installvariables.properties
-rwxr-xr-x    1 root     root remove.bssas.cron.sh*
-rwxrwxr-x    1 root     root remove.bssav.cron.sh*
```

```
-rw-rw-r--    1 root     root uninstaller.jar
```

./bin:

```
-r-xr-x---    1 mailwall bmi  av_cleaner*
-r-xr-x---    1 mailwall bmi  bmserver*
-r-xr-x---    1 mailwall bmi  conduit*
-r-xr-x---    1 mailwall bmi  harvester*
-r-xr-x---    1 mailwall bmi  kicker*
```

./bm_ruleset.2.avsym.1:

```
-rw-rw----    1 mailwall bmi  catalog.dat
-rw-rw----    1 mailwall bmi  navensol.so
-rw-rw----    1 mailwall bmi  navexsol.so
-rw-rw----    1 mailwall bmi  navupsol.dis
-rw-rw----    1 mailwall bmi  ncsacert.txt
-rw-rw----    1 mailwall bmi  scrauth.dat
-rw-rw----    1 mailwall bmi  technote.txt
-rw-rw----    1 mailwall bmi  tinf.dat
-rw-rw----    1 mailwall bmi  tinfidx.dat
-rw-rw----    1 mailwall bmi  tinfl.dat
-rw-rw----    1 mailwall bmi  tscan1.dat
-rw-rw----    1 mailwall bmi  tscan1hd.dat
-rw-rw----    1 mailwall bmi  update.txt
-rw-rw----    1 mailwall bmi  virscan.inf
-rw-rw----    1 mailwall bmi  virscan1.dat
-rw-rw----    1 mailwall bmi  virscan2.dat
-rw-rw----    1 mailwall bmi  virscan3.dat
-rw-rw----    1 mailwall bmi  virscan4.dat
-rw-rw----    1 mailwall bmi  virscan5.dat
-rw-rw----    1 mailwall bmi  virscan6.dat
-rw-rw----    1 mailwall bmi  virscan7.dat
-rw-rw----    1 mailwall bmi  virscan8.dat
-rw-rw----    1 mailwall bmi  virscan9.dat
-rw-rw----    1 mailwall bmi  whatsnew.txt
-rw-rw----    1 mailwall bmi  zdone.dat
```

./bm_ruleset.2.permit_rules.1:

```
-rw-rw----    1 mailwall bmi  permit_rules
```

./bm_ruleset.2.spamhunter_rules.1:

```
-rw-rw----    1 mailwall bmi  rules
```

./bm_ruleset.2.spamsig_rules.1:

```
-rw-rw----    1 mailwall bmi  spamsigs
```

./docs:

```
-rw-r--r--    1 mailwall bmi  documentation.html
```

./etc:

```
-r--r-----    1 mailwall bmi  AdvisoryStore.dtd
-rw-rw----    1 mailwall bmi  Notification.xml
-r--r--r--    1 mailwall bmi  agent.cert
-rw-rw-r--    1 mailwall bmi  agentconfig.xml
-r--r--r--    1 mailwall bmi  agent.key
drwxrwxr-x    2 mailwall bmi  bm_ruleset.2.avsym.1.sample/
-rw-rw-r--    1 mailwall bmi  bmiconfig.xml
-rwxrwxr-x    1 mailwall bmi  brightmail-env*
-r--r-----    1 mailwall bmi  hashes.sample
-rwx------    1 mailwall bmi  patchinstall*
-r--r-----    1 mailwall bmi  permit_rules.sample
-r-xr-x---    1 mailwall bmi  process-cleanup*
-r--r-----    1 mailwall bmi  rules.sample
-rw-rw-r--    1 mailwall bmi  runner.cfg
-rw-r-----    1 mailwall bmi  sieve_adult.sample
-rw-r-----    1 mailwall bmi  sieve_script.sample
-r--r-----    1 mailwall bmi  spamsigs.sample
drwxrwxr-x    2 mailwall bmi  tests/
-r--r--r--    1 mailwall bmi  trusted.cert
-rw-rw-r--    1 mailwall bmi  allowedblockedlist.txt
```

./etc/bm_ruleset.2.avsym.1.sample:

```
-rw-rw----    1 mailwall bmi  catalog.dat
-rw-rw----    1 mailwall bmi  navensol.so
-rw-rw----    1 mailwall bmi  navexsol.so
-rw-rw----    1 mailwall bmi  navupsol.dis
-rw-rw----    1 mailwall bmi  ncsacert.txt
-rw-rw----    1 mailwall bmi  scrauth.dat
-rw-rw----    1 mailwall bmi  technote.txt
```

```
-rw-rw----    1 mailwall bmi  tinf.dat
-rw-rw----    1 mailwall bmi  tinfidx.dat
-rw-rw----    1 mailwall bmi  tinfl.dat
-rw-rw----    1 mailwall bmi  tscan1.dat
-rw-rw----    1 mailwall bmi  tscan1hd.dat
-rw-rw----    1 mailwall bmi  update.txt
-rw-rw----    1 mailwall bmi  virscan.inf
-rw-rw----    1 mailwall bmi  virscan1.dat
-rw-rw----    1 mailwall bmi  virscan2.dat
-rw-rw----    1 mailwall bmi  virscan3.dat
-rw-rw----    1 mailwall bmi  virscan4.dat
-rw-rw----    1 mailwall bmi  virscan5.dat
-rw-rw----    1 mailwall bmi  virscan6.dat
-rw-rw----    1 mailwall bmi  virscan7.dat
-rw-rw----    1 mailwall bmi  virscan8.dat
-rw-rw----    1 mailwall bmi  virscan9.dat
-rw-rw----    1 mailwall bmi  whatsnew.txt
-rw-rw----    1 mailwall bmi  zdone.dat
```

./etc/tests:

```
drwxrwxr-x    2 mailwall bmi  lang_id/
-rw-r-----    1 mailwall bmi  rules.msg
-rw-r-----    1 mailwall bmi  sieve.adult.msg
-rw-r-----    1 mailwall bmi  sieve.sideline.msg
-rw-r-----    1 mailwall bmi  spamsig.msg
```

./etc/tests/lang_id:

```
-rw-r-----    1 mailwall bmi  de.eml
-rw-r-----    1 mailwall bmi  es.eml
-rw-r-----    1 mailwall bmi  fr.eml
-rw-r-----    1 mailwall bmi  it.eml
-rw-r-----    1 mailwall bmi  ja.eml
-rw-r-----    1 mailwall bmi  ko.eml
-rw-r-----    1 mailwall bmi  nl.eml
-rw-r-----    1 mailwall bmi  pt.eml
-rw-r-----    1 mailwall bmi  ru.eml
-rw-r-----    1 mailwall bmi  zh.eml
```

./jobs:

```
drwxr-x---    2 mailwall bmi  bmagent/
drwxr-x---    2 mailwall bmi  bmserver/
drwxr-x---    2 mailwall bmi  conduit/
drwxr-x---    2 mailwall bmi  harvester/
```

./jobs/bmagent:

./jobs/bmserver:

```
-rw-r-----    2 mailwall bmi  bmserver.stop
```

./jobs/conduit:

```
-rw-r-----    2 mailwall bmi  conduit.stop
```

./jobs/harvester:

```
-rw-r-----    2 mailwall bmi  harvester.stop
```

./lib:

```
-rwxr-xr-x    1 mailwall bmi  libACE.so.5.4.0*
lrwxrwxrwx    1 root     root libACE.so -> ./libACE.so.5.4.0*
-rwxr-xr-x    1 mailwall bmi  libACE_SSL.so.5.4.0*
lrwxrwxrwx    1 root     root libACE_SSL.so -> ./libACE_SSL.so.5.4.0*
-r--r-----    1 mailwall bmi  libantivirus.so
-r--r-----    1 mailwall bmi  libbh.so
-r-xr-x---    1 mailwall bmi  libbmishareddata.so*
-r-xr-x---    1 mailwall bmi  libbmiutil.so.1*
lrwxrwxrwx    1 root     root libicudata.so -> ./libicudata.so.28*
-rwxr-xr-x    1 mailwall bmi  libicudata.so.28*
lrwxrwxrwx    1 root     root libicui18n.so -> ./libicui18n.so.28*
-rwxr-xr-x    1 mailwall bmi  libicui18n.so.28*
lrwxrwxrwx    1 root     root libicuuc.so -> ./libicuuc.so.28*
-rwxr-xr-x    1 mailwall bmi  libicuuc.so.28*
-r--r-----    1 mailwall bmi  liblanguageid.so
-r--r-----    1 mailwall bmi  libpermit.so
-r--r-----    1 mailwall bmi  libregexfilter.so
-r--r-----    1 mailwall bmi  libreinsert.so
-r--r-----    1 mailwall bmi  libsieve.so
-r--r-----    1 mailwall bmi  libspamhunter.so
-r--r-----    1 mailwall bmi  libspamsig.so
-rwxr-xr-x    1 mailwall bmi  libstlport_gcc.so*
```

```
-rwxr-xr-x    1 mailwall bmi  libxml2.so.2*
lrwxrwxrwx    1 root     root libxml2.so -> ./libxml2.so.2*
```

./logs:

```
-rw-rw-r--    1 mailwall bmi  common_log
```

./stats:

```
-r-xr-x---    1 mailwall bmi  bmagent*
-r-xr-x---    1 mailwall bmi  controller.sh*
-r-xr-x---    1 mailwall bmi  inspector*
-r-xr-x---    1 mailwall bmi  register*
-r-xr-x---    1 mailwall bmi  register.sh*
-r-xr-x---    1 mailwall bmi  runcleaner.sh*
-r-xr-x---    1 mailwall bmi  runner*
-r-xr-x---    1 mailwall bmi  runcleaner.sh*
```

./stats:

Brightmail Scanner Installation with Brightmail Client Only

```
-rw-rw-r--    1 root     root Brightmail_Anti-Spam_InstallLog.log
-r--r--r--    1 mailwall bmi  EULA
-rw-r--r--    1 mailwall bmi  LEGAL.NOTICES.txt
drwxrwxr-x    2 root     root UninstallerData/
drwxr-x---    2 mailwall bmi  bin/
drwxr-xr-x    2 mailwall bmi  docs/
drwxr-xr-x    2 mailwall bmi  etc/
drwxr-x---    3 mailwall bmi  jobs/
drwxr-x---    2 mailwall bmi  lib/
drwxrwxr-x    2 mailwall bmi  logs/
drwxr-x---    2 mailwall bmi  sbin/
-rw-rw-r--    1 mailwall bmi  sieve_script.txt
```

./UninstallerData:

```
-rw-rw-r--    1 root     root InstallScript.iap_xml
-r-xr-x---    1 root     root Uninstall*
-rwxrwxr-x    1 root     root Uninstall.lax*
-rw-rw-r--    1 root     root installvariables.properties
-rw-rw-r--    1 root     root uninstaller.jar
```

./bin:

```
-rwxr-x---    1 mailwall bmi  bmifilter*
```

./docs:

```
-rw-r--r--    1 mailwall bmi  documentation.html
```

./etc:

```
-r--r--r--    1 mailwall bmi  agent.cert
-rw-rw-r--    1 mailwall bmi  agentconfig.xml
-r--r--r--    1 mailwall bmi  agent.key
-rw-rw-r--    1 mailwall bmi  bmiconfig.xml
-rwxrwxr-x    1 mailwall bmi  brightmail-env*
-rwx------    1 mailwall bmi  patchinstall*
-r-xr-x---    1 mailwall bmi  process-cleanup*
-rw-rw-r--    1 mailwall bmi  runner.cfg
```

./jobs:

```
drwxr-x---    2 mailwall bmi  bmagent/
drwxrwx---    2 mailwall bmi  bmifilter/
```

./jobs/bmagent:

./jobs/bmifilter:

```
-rw-r-----    2 mailwall bmi  bmifilter.stop
```

./lib:

```
-rwxr-xr-x    1 mailwall bmi  libACE.so.5.4.0*
lrwxrwxrwx    1 root     root libACE.so -> ./libACE.so.5.4.0*
-rwxr-xr-x    1 mailwall bmi  libACE_SSL.so.5.4.0*
lrwxrwxrwx    1 root     root libACE_SSL.so -> ./libACE_SSL.so.5.4.0*
-rwxr-xr-x    1 mailwall bmi  libbmiclient.so.1*
-r-xr-xr-x    1 mailwall bmi  libbmishareddata.so*
-r-xr-x---    1 mailwall bmi  libbmiutil.so.1*
-rwxr-xr-x    1 mailwall bmi  libstlport_gcc.so*
-rwxr-xr-x    1 mailwall bmi  libxml2.so.2*
lrwxrwxrwx    1 root     root libxml2.so -> ./libxml2.so.2*
```

./logs:

./sbin:

```
-r-xr-x---    1 mailwall bmi  bmagent*
```

```
-r-xr-x---    1 mailwall bmi  controller.sh*
-r-xr-x---    1 mailwall bmi  inspector*
-r-xr-x---    1 mailwall bmi  runner*
```

Brightmail Scanner on Windows

Brightmail Scanner, Complete (Brightmail Server, Brightmail Client)

C:\Program Files\Symantec\SBAS\Scanner

```
<DIR>          Bin
<DIR>          bmispool
<DIR>          bm_ruleset.2.avsym.1
<DIR>          bm_ruleset.2.permit_rules.1
<DIR>          bm_ruleset.2.spamhunter_rules.1
<DIR>          bm_ruleset.2.spamsig_rules.1
<DIR>          Config
<DIR>          Documentation
<DIR>          etc
<DIR>          Logs
<DIR>          Jobs
<DIR>          Spam
<DIR>          Stats
```

C:\Program Files\Symantec\SBAS\Scanner\Bin

```
ACE.dll
ACE_SSL.dll
av_cleaner.exe
bmagent.exe
bmiengine.dll
bmiEventLog.dll
bmiperf.dll
bmishareddata.dll
bmiSink52.dll
bmserver.exe
conduit.exe
Dec2.dll
Dec2AMG.dll
```

Dec2ARJ.dll
Dec2AS.dll
Dec2CAB.dll
Dec2EXE.dll
Dec2GHO.dll
Dec2GZIP.dll
Dec2HQX.dll
Dec2HTTP.dll
Dec2ID.dll
Dec2LHA.dll
Dec2LZ.dll
Dec2MB3.dll
Dec2MIME.dll
Dec2OLE1.dll
Dec2RAR.dll
Dec2RTF.dll
Dec2SS.dll
Dec2TAR.dll
Dec2Text.dll
Dec2TNEF.dll
Dec2UUE.dll
Dec2Zip.dll
DecSDK.dll
harvester.exe
icudt28l.dll
icuin28.dll
icuuc28.dll
kicker.exe
libantivirus.dll
libbh.dll
liblanguageid.dll
libpermit.dll
libregexfilter.dll
libreinsert.dll
libsieve.dll
libspamhunter.dll
libspamsig.dll

```
libxml2.dll
Navapi32.dll
Rec2.dll
regwizard.exe
stlport_vc646.dll
xerces-c_2_3_0.dll
```

C:\Program Files\Symantec\SBAS\Scanner\bmispool

```
<DIR>          spam
<DIR>          virus
```

C:\Program Files\Symantec\SBAS\Scanner\bmispool\spam

```
<DIR>          Badmail
```

C:\Program Files\Symantec\SBAS\Scanner\bmispool\spam\Badmail

C:\Program Files\Symantec\SBAS\Scanner\bmispool\virus

C:\Program Files\Symantec\SBAS\Scanner\bm_ruleset.2.avsym.1

```
CATALOG.DAT
FW15.DIS
IDUPGRAD.EXE
NAV40I.DIS
NAVENG.EXP
NAVENG.SYS
NAVENG.VXD
NAVENG32.DLL
NAVEX15.EXP
NAVEX15.SYS
NAVEX15.VXD
NAVEX32A.DLL
NCSACERT.TXT
SCRAUTH.DAT
SYMAVENG.CAT
SYMAVENG.INF
TECHNOTE.TXT
TINF.DAT
TINFIDX.DAT
TINFL.DAT
TSCAN1.DAT
```

TSCAN1HD.DAT
VIRSCAN.INF
VIRSCAN1.DAT
VIRSCAN2.DAT
VIRSCAN3.DAT
VIRSCAN4.DAT
VIRSCAN5.DAT
VIRSCAN6.DAT
VIRSCAN7.DAT
VIRSCAN8.DAT
VIRSCAN9.DAT
WHATSNEW.TXT
ZDONE.DAT

C:\Program Files\Symantec\SBAS\Scanner\bm_ruleset.2.permit_rules.1

permit_rules

C:\Program Files\Symantec\SBAS\Scanner\bm_ruleset.2.spamhunter_rules.1

rules

C:\Program Files\Symantec\SBAS\Scanner\bm_ruleset.2.spamsig_rules.1

spamsigs

C:\Program Files\Symantec\SBAS\Scanner\Config

agentconfig.xml
bmiconfig.xml
sieve_script.txt
allowedblockedlist.txt

C:\Program Files\Symantec\SBAS\Scanner\Documentation

documentation.html

C:\Program Files\Symantec\SBAS\Scanner\etc

AdvisoryStore.dtd
agent.cert
agent.key
BrightmailClient.H
BrightmailClient.ini
BrightmailModules.H
BrightmailModules.ini

```
BrightmailServer.H
BrightmailServer.ini
cert.pem
EULA.rtf
hashes.sample
<DIR>          tests
LEGAL.NOTICES.txt
Notification.xml
rules.sample
sieve_adult.txt
sieve_script.sample.txt
spamsigs.sample
trusted.cert
```

C:\Program Files\Symantec\SBAS\Scanner\etc\tests

```
<DIR>          lang_id
rules.msg
sieve.adult.msg
sieve.sideline.msg
spamsig.msg
```

C:\Program Files\Symantec\SBAS\Scanner\etc\tests\lang_id

```
de.eml
es.eml
fr.eml
it.eml
ja.eml
ko.eml
nl.eml
pt.eml
ru.eml
zh.eml
```

C:\Program Files\Symantec\SBAS\Scanner\Jobs

```
<DIR>          Bmserver
```

C:\Program Files\Symantec\SBAS\Scanner\Jobs\Bmserver

C:\Program Files\Symantec\SBAS\Scanner\Logs

C:\Program Files\Symantec\SBAS\Scanner\Spam

C:\Program Files\Symantec\SBAS\Scanner\Stats

Registry keys installed:

```
<*** ALL ***>
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\Application\Brightmail]
"EventMessageFile"="[INSTALLDIR]\Bin\bmiEventLog.dll"
"TypesSupported"=dword:00000007
"CategoryMessageFile"="[INSTALLDIR]\Bin\bmiEventLog.dll"
"CategoryCount"=dword:00000000

[HKEY_LOCAL_MACHINE\SOFTWARE\Brightmail]
"RTF"=dword:[BmiRuntimeFlags]
"ConfigFile"="[INSTALLDIR]\Config\bmiconfig.xml"
"LoadPoint"="[INSTALLDIR]"



<*** SERVER ***>
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\Application\Bright-
mailServer]
"EventMessageFile"="[INSTALLDIR]\bin\bmiPerf.dll"
"TypesSupported"=dword:00000007

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\Application\BrightmailMod-
ules]
"EventMessageFile"="[INSTALLDIR]\bin\bmiPerf.dll"
"TypesSupported"=dword:00000007

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\BrightmailServer]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\BrightmailServer\Performance]
"Library"="[INSTALLDIR]\bin\bmiPerf.dll"
"Open"="OpenData_Server"
"Collect"="CollectData_Server"
```

```
"Close"="CloseData_Server"
"Disable Performance Counters"=dword:00000000

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\BrightmailModules]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\BrightmailModules\Performance]
"Library"="[INSTALLDIR]\bin\bmiPerf.dll"
"Open"="OpenData_Modules"
"Collect"="CollectData_Modules"
"Close"="CloseData_Modules"
"Disable Performance Counters"=dword:00000000

[HKEY_LOCAL_MACHINE\SOFTWARE\Brightmail\Cleaner]
"Cleaner_interval"=dword:00000014

<*** CLIENT ***>

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\Application\BrightmailCli-
ent]
"EventMessageFile"="[INSTALLDIR]\bin\bmiPerf.dll"
"TypesSupported"=dword:00000007

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\BrightmailClient]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\BrightmailClient\Performance]
"Library"="[INSTALLDIR]\bin\bmiPerf.dll"
"Open"="OpenData_Client"
"Collect"="CollectData_Client"
"Close"="CloseData_Client"
"Disable Performance Counters"=dword:00000000

[HKEY_LOCAL_MACHINE\SOFTWARE\Brightmail\Sink]
"Thread_count"=dword:00000032
"Enabled"=dword:00000000
"Prop_GUID"="{23AA8321-27C4-4f24-B321-799A1B2A9E74}"
"Reload"=dword:00000000
"SMTPServerInstance"=dword:[SMTPVIRTSVR]
```

Brightmail Scanner Installation with Brightmail Server Only

C:\Program Files\Symantec\SBAS\Scanner

```
<DIR>          Bin
<DIR>          BmiSpool
<DIR>          bm_ruleset.2.avsym.1
<DIR>          bm_ruleset.2.permit_rules.1
<DIR>          bm_ruleset.2.spamhunter_rules.1
<DIR>          bm_ruleset.2.spamsig_rules.1
<DIR>          Config
<DIR>          Documentation
<DIR>          etc
<DIR>          Jobs
<DIR>          Logs
<DIR>          Spam
<DIR>          Stats
```

C:\Program Files\Symantec\SBAS\Scanner\Bin

```
ace.dll
ACE_SSL.dll
av_cleaner.exe
bmagent.exe
bmiengine.dll
bmiEventLog.dll
bmiperf.dll
bmishareddata.dll
bmserver.exe
conduit.exe
Dec2.dll
Dec2AMG.dll
Dec2ARJ.dll
Dec2AS.dll
Dec2CAB.dll
Dec2EXE.dll
Dec2GHO.dll
Dec2GZIP.dll
Dec2HQX.dll
Dec2HTTP.dll
```

Dec2ID.dll
Dec2LHA.dll
Dec2LZ.dll
Dec2MB3.dll
Dec2MIME.dll
Dec2OLE1.dll
Dec2RAR.dll
Dec2RTF.dll
Dec2SS.dll
Dec2TAR.dll
Dec2Text.dll
Dec2TNEF.dll
Dec2UUE.dll
Dec2Zip.dll
DecSDK.dll
harvester.exe
icudt28l.dll
icuin28.dll
icuuc28.dll
kicker.exe
libantivirus.dll
libbh.dll
liblanguageid.dll
libpermit.dll
libregexfilter.dll
libreinsert.dll
libsieve.dll
libspamhunter.dll
libspamsig.dll
libxml2.dll
Navapi32.dll
Rec2.dll
regwizard.exe
stlport_vc646.dll
xerces-c_2_3_0.dll

C:\Program Files\Symantec\SBAS\Scanner\BmiSpool

<DIR> Spam

```
<DIR>          Virus
```

C:\Program Files\Symantec\SBAS\Scanner\BmiSpool\Spam

```
<DIR>          Badmail
```

C:\Program Files\Symantec\SBAS\Scanner\BmiSpool\Virus

C:\Program Files\Symantec\SBAS\Scanner\bm_ruleset.2.avsym.1

```
CATALOG.DAT
FW15.DIS
IDUPGRAD.EXE
NAV40I.DIS
NAVENG.EXP
NAVENG.SYS
NAVENG.VXD
NAVENG32.DLL
NAVEX15.EXP
NAVEX15.SYS
NAVEX15.VXD
NAVEX32A.DLL
NCSACERT.TXT
SCRAUTH.DAT
SYMAVENG.CAT
SYMAVENG.INF
TECHNOTE.TXT
TINF.DAT
TINFIDX.DAT
TINFL.DAT
TSCAN1.DAT
TSCAN1HD.DAT
VIRSCAN.INF
VIRSCAN1.DAT
VIRSCAN2.DAT
VIRSCAN3.DAT
VIRSCAN4.DAT
VIRSCAN5.DAT
VIRSCAN6.DAT
VIRSCAN7.DAT
VIRSCAN8.DAT
```

```
VIRSCAN9.DAT
WHATSNEW.TXT
ZDONE.DAT
```

C:\Program Files\Symantec\SBAS\Scanner\bm_ruleset.2.permit_rules.1

```
permit_rules
```

C:\Program Files\Symantec\SBAS\Scanner\bm_ruleset.2.spamhunter_rules.1

```
rules
```

C:\Program Files\Symantec\SBAS\Scanner\bm_ruleset.2.spamsig_rules.1

```
spamsigs
```

C:\Program Files\Symantec\SBAS\Scanner\Config

```
agentconfig.xml
bmiconfig.xml
sieve_script.txt
allowedblockedlist.txt
```

C:\Program Files\Symantec\SBAS\Scanner\Documentation

```
documentation.html
```

C:\Program Files\Symantec\SBAS\Scanner\etc

```
AdvisoryStore.dtd
agent.cert
agent.key
BrightmailModules.H
BrightmailModules.ini
BrightmailServer.H
BrightmailServer.ini
EULA.rtf
hashes.sample
LEGAL.NOTICES.txt
Notification.xml
rules.sample
sieve_adult.txt
sieve_script.sample.txt
spamsigs.sample
<DIR>          tests
trusted.cert
```

C:\Program Files\Symantec\SBAS\Scanner\etc\tests

```
<DIR>          langid
rules.msg
sieve.adult.msg
sieve.sideline.msg
spamsig.msg
```

C:\Program Files\Symantec\SBAS\Scanner\etc\tests\langid

```
de.eml
es.eml
fr.eml
it.eml
ja.eml
ko.eml
nl.eml
pt.eml
ru.eml
zh.eml
```

C:\Program Files\Symantec\SBAS\Scanner\Jobs

```
<DIR>          Bmserver
```

C:\Program Files\Symantec\SBAS\Scanner\Jobs\Bmserver

C:\Program Files\Symantec\SBAS\Scanner\Logs

C:\Program Files\Symantec\SBAS\Scanner\Spam

C:\Program Files\Symantec\SBAS\Scanner\Stats

Registry keys installed:

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\Application\Brightmail]
"EventMessageFile"="[INSTALLDIR]\Bin\bmiEventLog.dll"
"TypesSupported"=dword:00000007
"CategoryMessageFile"="[INSTALLDIR]\Bin\bmiEventLog.dll"
"CategoryCount"=dword:00000000

[HKEY_LOCAL_MACHINE\SOFTWARE\Brightmail]
"RTF"=dword:[BmiRuntimeFlags]
"ConfigFile"="[INSTALLDIR]\Config\bmiconfig.xml"
"LoadPoint"="[INSTALLDIR]"
```

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\Application\Bright-
mailServer]
"EventMessageFile"="[INSTALLDIR]\bin\bmiPerf.dll"
"TypesSupported"=dword:00000007

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\Application\BrightmailMod-
ules]
"EventMessageFile"="[INSTALLDIR]\bin\bmiPerf.dll"
"TypesSupported"=dword:00000007

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\BrightmailServer]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\BrightmailServer\Performance]
"Library"="[INSTALLDIR]\bin\bmiPerf.dll"
"Open"="OpenData_Server"
"Collect"="CollectData_Server"
"Close"="CloseData_Server"
"Disable Performance Counters"=dword:00000000

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\BrightmailModules]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\BrightmailModules\Performance]
"Library"="[INSTALLDIR]\bin\bmiPerf.dll"
"Open"="OpenData_Modules"
"Collect"="CollectData_Modules"
"Close"="CloseData_Modules"
"Disable Performance Counters"=dword:00000000

[HKEY_LOCAL_MACHINE\SOFTWARE\Brightmail\Cleaner]
"Cleaner_interval"=dword:00000014
```

Brightmail Scanner Installation with Brightmail Client Only

C:\Program Files\Symantec\SBAS\Scanner

```
<DIR>          Bin
<DIR>          Config
<DIR>          Documentation
<DIR>          etc
```

```
<DIR>          Logs
```

C:\Program Files\Symantec\SBAS\Scanner\Bin

```
ace.dll
ACE_SSL.dll
bmagent.exe
bmiEventLog.dll
bmiperf.dll
bmishareddata.dll
bmiSink52.dll
libxml2.dll
stlport_vc646.dll
```

C:\Program Files\Symantec\SBAS\Scanner\Config

```
agentconfig.xml
bmiconfig.xml
```

C:\Program Files\Symantec\SBAS\Scanner\Documentation

```
documentation.html
```

C:\Program Files\Symantec\SBAS\Scanner\etc

```
agent.cert
agent.key
BrightmailClient.H
BrightmailClient.ini
EULA.rtf
LEGAL.NOTICES.txt
```

C:\Program Files\Symantec\SBAS\Scanner\Logs

Registry keys installed:

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\Application\Brightmail]
"EventMessageFile"="[INSTALLDIR]\Bin\bmiEventLog.dll"
"TypesSupported"=dword:00000007
"CategoryMessageFile"="[INSTALLDIR]\Bin\bmiEventLog.dll"
"CategoryCount"=dword:00000000

[HKEY_LOCAL_MACHINE\SOFTWARE\Brightmail]
"RTF"=dword:[BmiRuntimeFlags]
"ConfigFile"="[INSTALLDIR]\Config\bmiconfig.xml"
```

```
"LoadPoint"="[INSTALLDIR]"

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\Application\BrightmailCli-
ent]
"EventMessageFile"="[INSTALLDIR]\bin\bmiPerf.dll"
"TypesSupported"=dword:00000007

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\BrightmailClient]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\BrightmailClient\Performance]
"Library"="[INSTALLDIR]\bin\bmiPerf.dll"
"Open"="OpenData_Client"
"Collect"="CollectData_Client"
"Close"="CloseData_Client"
"Disable Performance Counters"=dword:00000000

[HKEY_LOCAL_MACHINE\SOFTWARE\Brightmail\Sink]
"Thread_count"=dword:00000032
"Enabled"=dword:00000000
"Prop_GUID"="{23AA8321-27C4-4f24-B321-799A1B2A9E74}"
"Reload"=dword:00000000
"SMTPServerInstance"=dword:[SMTPVIRTSVR]
```

Brightmail Control Center on All Platforms

```
-rw-rw-r--   1 root     root  BrightmailLog.log
-rw-rw-r--   1 root     root  Brightmail_Control_Center_InstallLog.log
drwxrwxr-x   3 root     root  MySQL
drwxrwxr-x   4 root     root  Tomcat
drwxrwxr-x   2 root     root  UninstallerData
-rwxrwxr-x   1 root     root  brightmail-env
-rw-r--r--   1 root     root  bq_admin_10.pdf
-rwxrwxr-x   1 root     root  uninstall.sh
-rwxrwxr-x   1 root     root  uninstall.bat
```

On UNIX, the MySQL directory is installed under the installation directory you choose, or in `/opt/symantec/SBAS/ControlCenter` if you choose the default directory.

On Windows, the MySQL directory is installed under `C:\mysql`.

./MySQL:

```
drwxr-xr-x  14 root     mysql  mysql-pro-4.0.16-sun-solaris2.8-sparc
-rwxrwxr-x   1 root     root   mysql-pro-4.0.16-sun-solaris2.8-sparc.tar
```

./MySQL/mysql-pro-4.0.16-sun-solaris2.8-sparc:

```
-rw-r--r--   1 root     mysql COPYING
-rw-r--r--   1 root     mysql COPYING.LIB
-rw-r--r--   1 root     mysql INSTALL-BINARY
-rw-r--r--   1 root     mysql MySQLEULA.txt
drwxr-xr-x   2 root     mysql bin
-rwxr-xr-x   1 root     mysql configure
drwxr-x---   5 mysql    mysql data
drwxr-xr-x   2 root     mysql docs
drwxr-xr-x   2 root     mysql include
drwxr-xr-x   2 root     mysql lib
drwxr-xr-x   3 root     mysql man
drwxr-xr-x   6 root     mysql mysql-test
drwxr-xr-x   2 root     mysql scripts
drwxr-xr-x   3 root     mysql share
drwxr-xr-x   5 root     mysql sql-bench
drwxr-xr-x   2 root     mysql support-files
drwxr-xr-x   2 root     mysql tests
```

./MySQL/mysql-pro-4.0.16-sun-solaris2.8-sparc/bin:

```
-rwxr-xr-x  1 root   mysql comp_err
-rwxr-xr-x  1 root   mysql isamchk
-rwxr-xr-x  1 root   mysql make_sharedlib_distribu
-rwxr-xr-x  1 root   mysql make_win_src_distributi
-rwxr-xr-x  1 root   mysql msql2mysql
-rwxr-xr-x  1 root   mysql my_print_defaults
-rwxr-xr-x  1 root   mysql myisamchk
-rwxr-xr-x  1 root   mysql myisamlog
-rwxr-xr-x  1 root   mysql myisampack
-rwxr-xr-x  1 root   mysql mysql
-rwxr-xr-x  1 root   mysql mysql_config
-rwxr-xr-x  1 root   mysql mysql_convert_table_for
```

```
-rwxr-xr-x  1 root    mysql mysql_explain_log
-rwxr-xr-x  1 root    mysql mysql_find_rows
-rwxr-xr-x  1 root    mysql mysql_fix_extensions
-rwxr-xr-x  1 root    mysql mysql_fix_privilege_tab
-rwxr-xr-x  1 root    mysql mysql_secure_installati
-rwxr-xr-x  1 root    mysql mysql_setpermission
-rwxr-xr-x  1 root    mysql mysql_tableinfo
-rwxr-xr-x  1 root    mysql mysql_waitpid
-rwxr-xr-x  1 root    mysql mysql_zap
-rwxr-xr-x  1 root    mysql mysqlaccess
-rwxr-xr-x  1 root    mysql mysqlaccess.conf
-rwxr-xr-x  1 root    mysql mysqladmin
-rwxr-xr-x  1 root    mysql mysqlbinlog
-rwxr-xr-x  1 root    mysql mysqlbug
-rwxr-xr-x  1 root    mysql mysqlcheck
-rwxr-xr-x  1 root    mysql mysqld
-rwxr-xr-x  1 root    mysql mysqld.sym.gz
-rwxr-xr-x  1 root    mysql mysqld_multi
-rwxr-xr-x  1 root    mysql mysqld_safe
-rwxr-xr-x  1 root    mysql mysqldump
-rwxr-xr-x  1 root    mysql mysqldumpslow
-rwxr-xr-x  1 root    mysql mysqlhotcopy
-rwxr-xr-x  1 root    mysql mysqlimport
-rwxr-xr-x  1 root    mysql mysqlmanager
-rwxr-xr-x  1 root    mysql mysqlmanager-pwgen
-rwxr-xr-x  1 root    mysql mysqlmanagerc
-rwxr-xr-x  1 root    mysql mysqlshow
-rwxr-xr-x  1 root    mysql mysqltest
-rwxr-xr-x  1 root    mysql pack_isam
-rwxr-xr-x  1 root    mysql perror
-rwxr-xr-x  1 root    mysql replace
-rwxr-xr-x  1 root    mysql resolve_stack_dump
-rwxr-xr-x  1 root    mysql resolveip
lrwxrwxrwx   1 105      other safe_mysqld -> mysqld_safe
```

./MySQL/mysql-pro-4.0.16-sun-solaris2.8-sparc/data:

```
drwx------   2 mysql    mysql brightmail
```

```
-rw-rw----   1 mysql    mysql ib_arch_log_0000000000
-rw-rw----   1 mysql    mysql ib_logfile0
-rw-rw----   1 mysql    mysql ib_logfile1
-rw-rw----   1 mysql    mysql ibdata1
-rwxrwxr-x   1 mysql    mysql my.cnf
drwxr-x---   2 mysql    mysql mysql
-rw-rw----   1 mysql    root  host.err
-rw-rw----   1 mysql    mysql host.pid
drwxr-x---   2 mysql    mysql test
```

./MySQL/mysql-pro-4.0.16-sun-solaris2.8-sparc/data/mysql:

```
-rw-rw----   1 mysql    mysql columns_priv.MYD
-rw-rw----   1 mysql    mysql columns_priv.MYI
-rw-rw----   1 mysql    mysql columns_priv.frm
-rw-rw----   1 mysql    mysql db.MYD
-rw-rw----   1 mysql    mysql db.MYI
-rw-rw----   1 mysql    mysql db.frm
-rw-rw----   1 mysql    mysql func.MYD
-rw-rw----   1 mysql    mysql func.MYI
-rw-rw----   1 mysql    mysql func.frm
-rw-rw----   1 mysql    mysql host.MYD
-rw-rw----   1 mysql    mysql host.MYI
-rw-rw----   1 mysql    mysql host.frm
-rw-rw----   1 mysql    mysql tables_priv.MYD
-rw-rw----   1 mysql    mysql tables_priv.MYI
-rw-rw----   1 mysql    mysql user.frm
-rw-rw----   1 mysql    mysql tables_priv.frm
-rw-rw----   1 mysql    mysql user.MYD
-rw-rw----   1 mysql    mysql user.MYI
```

./MySQL/mysql-pro-4.0.16-sun-solaris2.8-sparc/docs:

```
-rw-r--r--   1 root     mysql ChangeLog
-rw-r--r--   1 root     mysql manual.html
-rw-r--r--   1 root     mysql manual.txt
-rw-r--r--   1 root     mysql manual_toc.html
```

```
-rw-r--r--   1 root     mysql mysql.info
```

ql-pro-4.0.16-sun-solaris2.8-sparc/lib:

```
-rw-r--r--   1 root     mysql libdbug.a
-rw-r--r--   1 root     mysql libmygcc.a
-rw-r--r--   1 root     mysql libmysqlclient.a
-rw-r--r--   1 root     mysql libmysqlclient_r.a
-rw-r--r--   1 root     mysql libmysqld.a
-rw-r--r--   1 root     mysql libmystrings.a
-rw-r--r--   1 root     mysql libmysys.a
```

./MySQL/mysql-pro-4.0.16-sun-solaris2.8-sparc/scripts:

```
-rwxrwxr-x   1 root     mysql brightmail.sql
-rwxrwxr-x   1 root     mysql brightmail_create_db.sql
-rwxrwxr-x   1 root     mysql brightmail_create_tables.sql
-rwxrwxr-x   1 root     mysql brightmail_drop_tables.sql
-rwxrwxr-x   1 root     mysql brightmail_load_data.sql
-rwxrwxr-x   1 root     mysql brightmail_rename_tables.sql
-rwxrwxr-x   1 root     mysql mysql_install_db
```

./MySQL/mysql-pro-4.0.16-sun-solaris2.8-sparc/share:

```
drwxr-xr-x  25 root     mysql mysql
```

./MySQL/mysql-pro-4.0.16-sun-solaris2.8-sparc/support-files:

```
-rw-r--r--   1 root    mysql  MySQL-shared-compat.spec
-rw-r--r--   1 root     mysql  magic
-rw-r--r--   1 root     mysql  my-huge.cnf
-rw-r--r--   1 root     mysql  my-large.cnf
-rw-r--r--   1 root     mysql  my-medium.cnf
-rw-r--r--   1 root     mysql  my-small.cnf
-rwxr-xr-x   1 root     mysql  mysql-4.0.16.spec
-rwxr-xr-x   1 root     mysql  mysql-log-rotate
-rwxr-xr-x   1 root     mysql  mysql.server
-rw-r--r--   1 root     mysql  mysql.spec
```

./Tomcat:

```
drwxr-xr-x  11 root     root  jakarta-tomcat-4.1.27
-rwxrwxr-x   1 root     root  tomcat-4.1.27.zip
```

./Tomcat/jakarta-tomcat-4.1.27:

```
-rw-r--r--   1 root     root  LICENSE
-rw-r--r--   1 root     root  README.txt
-rw-r--r--   1 root     root  RELEASE-NOTES-4.1.txt
-rw-r--r--   1 root     root  RELEASE-PLAN-4.1.txt
-rw-r--r--   1 root     root  RUNNING.txt
drwxr-xr-x   2 root     root  bin
-rw-rw-r--   1 root     root  catalina_pid
drwxr-xr-x   5 root     root  common
drwxr-xr-x   2 root     root  conf
drwxr-xr-x   2 root     root  logs
drwxr-xr-x   5 root     root  server
drwxr-xr-x   4 root     root  shared
drwxr-xr-x   2 root     root  temp
drwxr-xr-x   7 root     root  webapps
drwxr-xr-x   3 root     root  work
```

./Tomcat/jakarta-tomcat-4.1.27/bin:

```
-rw-r--r--   1 root     root  bootstrap.jar
-rw-r--r--   1 root     root  catalina.bat
-rwxr-xr-x   1 root     root  catalina.sh
-rw-r--r--   1 root     root  commons-daemon.jar
-rw-r--r--   1 root     root  cpappend.bat
-rw-r--r--   1 root     root  digest.bat
-rwxr-xr-x   1 root     root  digest.sh
-rw-r--r--   1 root     root  jasper.bat
-rwxr-xr-x   1 root     root  jasper.sh
-rw-r--r--   1 root     root  jspc.bat
-rwxr-xr-x   1 root     root  jspc.sh
-rw-r--r--   1 root     root  setclasspath.bat
-rwxrwxr-x   1 root     root  setclasspath.sh
-rw-r--r--   1 root     root  shutdown.bat
```

```
-rwxr-xr-x   1 root     root  shutdown.sh
-rw-r--r--   1 root     root  startup.bat
-rwxr-xr-x   1 root     root  startup.sh
-rw-r--r--   1 root     root  tomcat-jni.jar
-rw-r--r--   1 root     root  tomcat.exe
-rw-r--r--   1 root     root  tool-wrapper.bat
-rwxr-xr-x   1 root     root  tool-wrapper.sh
```

./Tomcat/jakarta-tomcat-4.1.27/common:

```
drwxr-xr-x   2 root     root  classes
drwxr-xr-x   2 root     root  endorsed
drwxr-xr-x   2 root     root  lib
```

./Tomcat/jakarta-tomcat-4.1.27/common/classes:

./Tomcat/jakarta-tomcat-4.1.27/common/endorsed:

```
-rw-r--r--   1 root     root  xercesImpl.jar
-rw-r--r--   1 root     root  xmlParserAPIs.jar
```

./Tomcat/jakarta-tomcat-4.1.27/common/lib:

```
-rw-r--r--  1 root    root  activation.jar
-rw-r--r--  1 root    root  ant.jar
-rw-r--r--  1 root    root  commons-collections.jar
-rw-r--r--  1 root    root  commons-dbcp.jar
-rw-r--r--  1 root    root  commons-logging-api.jar
-rw-r--r--  1 root    root  commons-pool.jar
-rw-r--r--  1 root    root  jasper-compiler.jar
-rw-r--r--  1 root    root  jasper-runtime.jar
-rw-r--r--  1 root    root  jdbc2_0-stdext.jar
-rw-r--r--  1 root    root  jndi.jar
-rw-r--r--  1 root    root  jta.jar
-rw-r--r--  1 root    root  mail.jar
-rwxrwxr-x  1 root    root mysql-connector-java-com-3.0.11-stable-bin.jar
-rw-r--r--  1 root    root  naming-common.jar
-rw-r--r--  1 root    root  naming-factory.jar
-rw-r--r--  1 root    root  naming-resources.jar
```

```
-rw-r--r--   1 root    root  servlet.jar
```

./Tomcat/jakarta-tomcat-4.1.27/conf:

```
-rw-r--r--   1 root     root  catalina.policy
-rw-r--r--   1 root     root  jk2.properties
-rw-r--r--   1 root     root  server-noexamples.xml.config
-rwxrwxr-x   1 root     root  server.xml
-rw-rw-r--   1 root     root  tomcat-users.xml
-rw-r--r--   1 root     root  web.xml
```

./Tomcat/jakarta-tomcat-4.1.27/logs:

```
-rw-rw-r--   1 root     root  catalina.out
-rw-rw-r--   1 root     root  localhost_Brightmail_log.2004-03-09.txt
-rw-rw-r--   1 root     root  localhost_admin_log.2004-03-09.txt
-rw-rw-r--   1 root     root  localhost_log.2004-03-09.txt
```

./Tomcat/jakarta-tomcat-4.1.27/server:

```
drwxr-xr-x   2 root     root  classes
drwxr-xr-x   2 root     root  lib
drwxr-xr-x   4 root     root  webapps
```

./Tomcat/jakarta-tomcat-4.1.27/server/classes:

./Tomcat/jakarta-tomcat-4.1.27/server/lib:

```
-rw-r--r--   1 root     root  catalina-ant.jar
-rw-r--r--   1 root     root  catalina.jar
-rw-r--r--   1 root     root  commons-beanutils.jar
-rw-r--r--   1 root     root  commons-digester.jar
-rw-r--r--   1 root     root  commons-fileupload-1.0.jar
-rw-r--r--   1 root     root  commons-logging.jar
-rw-r--r--   1 root     root  commons-modeler.jar
-rw-r--r--   1 root     root  jaas.jar
-rw-r--r--   1 root     root  jakarta-regexp-1.2.jar
-rw-r--r--   1 root     root  mx4j-jmx.jar
-rw-r--r--   1 root     root  mx4j.license
-rw-r--r--   1 root     root  servlets-cgi.renametojar
```

```
-rw-r--r--   1 root     root  servlets-common.jar
-rw-r--r--   1 root     root  servlets-default.jar
-rw-r--r--   1 root     root  servlets-invoker.jar
-rw-r--r--   1 root     root  servlets-manager.jar
-rw-r--r--   1 root     root  servlets-ssi.renametojar
-rw-r--r--   1 root     root  servlets-webdav.jar
-rw-r--r--   1 root     root  tomcat-coyote.jar
-rw-r--r--   1 root     root  tomcat-http11.jar
-rw-r--r--   1 root     root  tomcat-jk.jar
-rw-r--r--   1 root     root  tomcat-jk2.jar
-rw-r--r--   1 root     root  tomcat-util.jar
-rw-r--r--   1 root     root  tomcat-warp.jar
```

./Tomcat/jakarta-tomcat-4.1.27/server/webapps:

```
drwxr-xr-x  15 root     root  admin
drwxr-xr-x   4 root     root  manager
```

./Tomcat/jakarta-tomcat-4.1.27/server/webapps/brightmail:

All `brightmail` files go here after the `brightmail.war` file is exploded

./Tomcat/jakarta-tomcat-4.1.27/work:

```
drwxrwxr-x   3 root     root  Standalone
```

./Tomcat/jakarta-tomcat-4.1.27/work/Standalone:

```
drwxrwxr-x   9 root     root  localhost
```

./Tomcat/jakarta-tomcat-4.1.27/work/Standalone/localhost:

```
drwxrwxr-x   2 root     root  _
drwxrwxr-x   2 root     root  admin
drwxrwxr-x   2 root     root  brightmail
drwxrwxr-x   2 root     root  examples
drwxrwxr-x   2 root     root  manager
drwxrwxr-x   2 root     root  tomcat-docs
drwxrwxr-x   2 root     root  webdav
```

./UninstallerData:

```
-rw-rw-r--   1 root     root  InstallScript.iap_xml
-rwxr-xr-x   1 root     root  Uninstall_Brightmail_Control_Center
-rwxrwxr-x   1 root     root  Uninstall_Brightmail_Control_Center.lax
-rw-rw-r--   1 root     root  installvariables.properties
-rw-rw-r--   1 root     root  uninstaller.jar
```

Appendix B: Third Party Licenses

This Appendix contains the licenses and notices for third-party software used in Symantec Brightmail AntiSpam.

ACE

Symantec Brightmail AntiSpam uses the ADAPTIVE Communication Environment (ACE[TM]) libraries maintained by the Center for Distributed Object Computing of Washington University. Copyright and Licensing Information for ACE[TM] and TAO[TM]

ACE[TM] and TAO[TM] are copyrighted by Douglas C. Schmidt and his research group at Washington University and University of California, Irvine

¬ Copyright 1993-2001, all rights reserved. Since ACE and TAO are open-source, free software, you are free to use, modify, copy, and distribute--perpetually and irrevocably--the ACE and TAO source code and object code produced from the source, as well as copy and distribute modified versions of this software. However, you must

include this copyright statement along with code built using ACE and TAO. In particular, you can use ACE and TAO in proprietary software and are under no obligation to redistribute any of your source code that is built using ACE and TAO. Note, however, that you may not do anything to the ACE and TAO code, such as copyrighting it yourself or claiming authorship of the ACE and TAO code, that will prevent ACE and TAO from being distributed freely using an open-source development model.

ACE and TAO are provided as is with no warranties of any kind, including the warranties of design, merchantability, and fitness for a particular purpose, noninfringement, or arising from a course of dealing, usage or trade practice. Moreover, ACE and TAO are provided with no support and without any obligation on the part of Washington

University, UC Irvine, their employees, or students to assist in its use, correction, modification, or enhancement. However, commercial support for ACE and TAO are available from Riverace and OCI, respectively. Moreover, both ACE and TAO are Y2K-compliant, as long as the underlying OS platform is Y2K-compliant.

Washington University, UC Irvine, their employees, and students shall have no liability with respect to the infringement of copyrights, trade secrets or any patents by ACE and TAO or any part thereof. Moreover, in no event will Washington University or UC Irvine, their employees, or students be liable for any lost revenue or profits or

other special, indirect and consequential damages.

The ACE and TAO web sites are maintained by the Center for Distributed Object Computing of Washington University for the development of open-source software as part of the open-source software community. By submitting comments, suggestions, code, code snippets, techniques (including that of usage), and algorithms, submitters acknowledge that they have the right to do so, that any such submissions are givenfreely and unreservedly, and that they waive any claims to copyright or ownership. In addition, submitters acknowledge that any such submission might become part of the copyright maintained on the overall body of code, which comprises the ACE and TAO software. By making a submission, submitter agree to these terms. Furthermore, submitters acknowledge that the incorporation or modification of such submissions is entirely at the discretion of the moderators of the open-source ACE and TAO projects or their designees.

The names ACE[TM], TAO[TM], Washington University, and UC Irvine, may not be used to endorse or promote products or services derived from this source without express written permission from Washington University or UC Irvine. Further, products or services derived from this source may not be called ACE[TM] or TAO[TM], nor may the name Washington University or UC Irvine appear in their names, without express written permission from Washington University or UC Irvine.

If you have any suggestions, additions, comments, or questions, please contact Douglas C. Schmidt at schmidt@cs.wustl.edu.

Apache Software Foundation: Apache HTTP Server, Xerces 2.1, Jakarta Tomcat

This product includes portions of the Apache Web Server software, developed by the Apache Software Foundation (http://www.apache.org/).

The Apache Software License, Version 1.1

Copyright (c) 1999 The Apache Software Foundation. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met: 1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer. 2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution. 3. The end-user documentation included with the redistribution, if any, must include the following acknowledgment: "This product includes software developed by the Apache Software Foundation (http://www.apache.org/)." Alternately, this acknowledgment may appear in the software itself, if and wherever such third-party acknowledgments normally appear. 4. The names "Apache", "log4j", "Xerces", and "Apache Software Foundation" must not be used to endorse or promote products derived from this software without prior written permission.For written permission, please contact apache@apache.org. 5. Products derived from this software may not be called "Apache", nor may "Apache" appear in their name, without prior written permission of the Apache Software Foundation. THIS SOFTWARE IS PROVIDED ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE APACHE SOFTWARE FOUNDATION OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT,

INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE. This software consists of voluntary contributions made by many individuals on behalf of the Apache Software Foundation and was originally based on software copyright (c) 1999, International Business Machines, Inc., http://www.ibm.com. Portions of this software are based upon public domain software originally written at the National Center for Supercomputing Applications, University of Illinois, Urbana-Champaign. For more information on the Apache Software Foundation, please see http://www.apache.org/.

Apache Portable Run-time

==========

Symantec Brightmail AntiSpam contains software derived from the Apache Portable Runtime function, which is derived from software contributed to Berkeley by Guido van Rossum:

Copyright (c) 1989, 1993, 1994

The Regents of the University of California.

All rights reserved.

Symantec Brightmail AntiSpam contains software derived from the BSD stdio library, which is derived from software contributed to Berkeley by Chris Torek:

Copyright (c) 1990, 1993

The Regents of the University of California. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Date Picker

The Brightmail Control Center software uses Date Picker, a freeware calendar application created by Wing Lee, available at http://64.246.32.44/~admin59/index.htm.

DES

Symantec Brightmail AntiSpam includes an implementation of DES developed by Eric Young (eay@cryptsoft.com). ¬ 1995-1997 Eric Young (eay@cryptsoft.com). All rights reserved. This package is a DES implementation written by Eric Young (eay@cryptsoft.com). The implementation was written so as to conform with MIT's libdes. This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution. Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the SSL library. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer. 2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution. 3. All advertising materials mentioning features or use of this software must display the following acknowledgement: This product includes software developed by Eric Young (eay@cryptsoft.com).

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The license and distribution terms for any publicly available version or derivative of this code cannot be changed. i.e., this code cannot simply be copied and put under another distribution license [including the GNU Public License.] The reason behind this being stated in this direct manner is past experience in code simply being copied and the attribution removed from it and then being distributed as part of other packages. This implementation was a non-trivial and unpaid effort.

International Components for UNICODE (ICU) Version 2.8

COPYRIGHT AND PERMISSION NOTICE

Copyright (c) 1995-2003 International Business Machines Corporation and others All rights reserved.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, provided that the above copyright notice(s) and this permission notice appear in all copies of the Software and that both the above copyright notice(s) and this permission notice appear in supporting documentation.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF THIRD PARTY RIGHTS. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR HOLDERS INCLUDED IN THIS NOTICE BE LIABLE FOR ANY CLAIM, OR ANY SPECIAL INDIRECT OR CONSEQUENTIAL DAMAGES, OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Except as contained in this notice, the name of a copyright holder shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Software without prior written authorization of the copyright holder. All trademarks and registered trademarks mentioned herein are the property of their respective owners.

Jikes

he Brightmail Control Center software contains and uses the Jikes[TM] compiler, which is Copyright ¬ 2003-2004, International Business Machines Corporation and others. All Rights Reserved. Jikes(c) is available at http://www-124.ibm.com/developerworks/opensource/jikes/

libxml2

Symantec Brightmail AntiSpam includes portions of the libxml2 library, found at http://www.xmlsoft.org/.

Except where otherwise noted in the source code (e.g. the files hash.c, list.c and the trio files, which are covered by a similar licence but with different Copyright notices) all the files are: Copyright (C) 1998-2003 Daniel Veillard. All Rights Reserved. Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is fur- nished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FIT- NESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE DANIEL VEILLARD BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CON- NECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Except as contained in this notice, the name of Daniel Veillard shall not be used in advertising or otherwise to promote the sale, use or other deal- ings in this Software without prior written authorization from him. the hash.c, list.c, and trio files are licensed as follows:

* Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

* THIS SOFTWARE IS PROVIDED ``AS IS'' AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTIBILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE AUTHORS AND CONTRIBUTORS ACCEPT NO RESPONSIBILITY IN ANY CONCEIVABLE MANNER.

hash.c is: Copyright (C) 2000 Bjorn Reese and Daniel Veillard. Author: breese@users.sourceforge.net

list.c is: Copyright (C) 2000 Gary Pennington and Daniel Veillard. Author: Gary.Pennington@uk.sun.com

the trio files (http://ctrio.sourceforge.net/ are: trio.c: * Copyright (C) 1998 Bjorn Reese and Daniel Stenberg. trio.h: * Copyright (C) 1998 Bjorn Reese and Daniel Stenberg. triodef.h: * Copyright (C) 2001 Bjorn Reese <breese@users.sourceforge.net> trionan.c: * Copyright (C) 2001 Bjorn Reese <breese@users.sourceforge.net> trionan.h: * Copyright (C) 2001 Bjorn Reese <breese@users.sourceforge.net> triop.h: * Copyright (C) 2000 Bjorn Reese and Daniel Stenberg. triostr.c: * Copyright (C) 2001 Bjorn Reese and Daniel Stenberg. triostr.h: * Copyright (C) 2001 Bjorn Reese and Daniel Stenberg.

MD5 Message-Digest Algorithm

Symantec Brightmail AntiSpam contains software derived from the RSA Data Security, Inc. MD5 Message-Digest Algorithm, which is (c) 1991, 1992 RSA Data Security, Inc. Created 1991. All rights reserved. MD5 is a registered trademark of RSA Data Security, Inc.

MySQL

The Brightmail Control Center software contains the Commercial (non-GPL) MySQL(c) software whose copyright is owned by, or licensed from MySQL AB (http://www.mysql.com/).

OpenSSL and Original SSLeay

Symantec Brightmail AntiSpam uses OpenSSL SSL/TLS and cryptographic libraries created and maintained by the OpenSSL Project (http://www.openssl.org).

LICENSE ISSUES ----------

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org. OpenSSL License ---------- Copyright (c) 1998-2001 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer. 2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution. 3. All advertising materials mentioning features or use of this software must display the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)" 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org. 5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project. 6. Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT \``AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE. ----------

This product includes cryptographic software written by EricYoung (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License----------

Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com) All rights reserved. This package is an SSL implementation written by Eric Young (eay@cryptsoft.com). The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are aheared to. The following conditions apply to all code found in this distribution, be it the RC4, RSA,lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms

except that the holder is Tim Hudson (tjh@cryptsoft.com). Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met: 1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer. 2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution. 3. All advertising materials mentioning features or use of this software must display the following acknowledgement: "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)" The word 'cryptographic' can be left out if the rouines from the library being used are not cryptographic related :-). 4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG \``AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The licence and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution licence [including the GNU Public Licence.]

parseaddr

Symantec Brightmail AntiSpam contains software derived from CMU's RFC 822 address parser, which is developed by Computing Services at Carnegie Mellon University (http://www.cmu.edu/computing/).

Copyright (c) 1998-2000 Carnegie Mellon University. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. The name "Carnegie Mellon University" must not be used to endorse or promote products derived from this software without prior written permission. For permission or any other legal details, please contact:

Office of Technology Transfer

Carnegie Mellon University

5000 Forbes Avenue

Pittsburgh, PA 15213-3890

(412) 268-4387, fax: (412) 268-7395

tech-transfer@andrew.cmu.edu

4. Redistributions of any form whatsoever must retain the following acknowledgment:

"This product includes software developed by Computing Services at Carnegie Mellon University (http://www.cmu.edu/computing/)."

CARNEGIE MELLON UNIVERSITY DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS, IN NO EVENT SHALL CARNEGIE MELLON UNIVERSITY BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

PCRE

This product contains regular expression support provided in part by the PCRE library package, which is open source software, written by Philip Hazel, and copyright by the University of Cambridge, England: Copyright (c) 1997-2001 University of Cambridge PCRE can be obtained here: ftp://ftp.csx.cam.ac.uk/pub/software/programming/pcre/

Quartz Enterprise Job Scheduler

The Brightmail Control Center software uses the Quartz Enterprise Job Scheduler, which is Copyright James House ¬ 2001-2003 All rights reserved.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

SpamAssassin

Symantec Brightmail AntiSpam contains software derived from SpamAssassin (http://www.spamassassin.org/), and is used here under Perl's Artistic License. Portions of SpamAssassin were converted from Perl to C. SpamAssassin is Copyright 2000-2002, Justin Mason (jm@jmason.org). All rights reserved.

The original work on SpamAssassin can be obtained here: http://www.spamassassin.org/downloads.html

The "Perl Artistic License"

Preamble The intent of this document is to state the conditions under which the Perl Package may be copied, such that the Copyright Holder maintains some semblance of artistic control over its development, while giving Perl users the right to use and distribute Perl in a more-or-less customary fashion, plus the right to make reasonable modifications.

Definitions:

"Package" refers to the collection of Perl-kit files distributed by the Copyright Holder, and derivatives of that collection of files created through textual modification. "Standard Version" refers to such a Package if it has not been modified, or has been modified as specified below. "Copyright Holder" is whoever is named in the copyright or copyrights for the Perl package. "You" is you, if you're thinking about copying or distributing this Package. "Reasonable copying fee" is whatever you can justify on the basis of media cost, duplication charges, time of people involved, and so on. (You will not be required to justify it to the Copyright Holder, but only to the computing community at large as a market that must bear the fee.) "Freely Available" means that no fee is charged for the item itself, though there may be fees involved in handling the item. It also means that recipients of the item may redistribute it under the same conditions they received it.

1. You may make and give away verbatim copies of the source form of the Standard Version of this Perl Package without restriction, provided that you duplicate all of the original copyright notices and associated disclaimers. 2. You may apply bug fixes, portability fixes and other modifications derived from the Public Domain or from the Copyright Holder. A Package modified in such a way shall still be considered the Standard Version. 3. You may otherwise modify your copy of this Perl Package in any way,

provided that you insert a prominent notice in each changed file stating how and when you changed that file, and provided that you do at least ONE of the following: a) place your modifications in the Public Domain or otherwise make them Freely Available, such as by posting said modifications to Usenet or an equivalent medium, or placing the modifications on a major archive site such as uunet.uu.net, or by allowing the Copyright Holder to include your modifications in the Standard Version of the Perl Package. b) use the modified Perl Package only within your corporation or organization. c) rename any non-standard executables so the names do not conflict with standard executables, which must also be provided, and provide a separate manual page for each non-standard executable that clearly documents how it differs from the Standard Version. d) make other distribution arrangements with the Copyright Holder. 4. You may distribute the programs of this Perl Package in object code or executable form, provided that you do at least ONE of the following: a) distribute a Standard Version of the executables and library files, together with instructions (in the manual page or equivalent) on where to get the Standard Version. b) accompany the distribution with the machine-readable source of the Perl Package with your modifications. c) accompany any non-standard executables with their corresponding Standard Version executables, giving the non-standard executables non-standard names, and clearly documenting the differences in manual pages (or equivalent), together with instructions on where to get the Standard Version. d) make other distribution arrangements with the Copyright Holder. 5. You may charge a reasonable copying fee for any distribution of this Perl Package. You may charge any fee you choose for support of this Perl Package. You may not charge a fee for this Perl Package itself. However, you may distribute this Perl Package in aggregate with other (possibly commercial) programs as part of a larger (possibly commercial) software distribution provided that you do not advertise this Perl Package as a product of your own. 6. The scripts and library files supplied as input to or produced as output from the programs of this Perl Package do not automatically fall under the copyright of this Perl Package, but belong to whomever generated

them, and may be sold commercially, and may be aggregated with this Perl Package. 7. C subroutines supplied by you and linked into this Perl Package in order to emulate subroutines and variables of the language defined by this Perl Package shall not be considered part of this Perl Package, but are the equivalent of input as in Paragraph 6, provided these subroutines do not change the language in any way that would cause it to fail the regression tests for the language. 8. The name of the Copyright Holder may

not be used to endorse or promote products derived from this software without specific prior written permission. 9. This PERL PACKAGE IS PROVIDED "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTIBILITY AND FITNESS FOR A PARTICULAR PURPOSE. The End

STLport

The Brightmail Control Center software uses the multiplatform ANSI C++ Standard Library implementation, STLport. STLport was modified slightly to provide compatibility with the ACEÖ library. Copyright ¬ 1999, 2000 Boris Fomitchev

This material is provided "as is", with absolutely no warranty expressed or implied. Any use is at your own risk. Permission to use or copy this software for any purpose is hereby granted without fee, provided the above notices are retained on all copies. Permission to modify the code and to distribute modified code is granted, provided the above notices are retained, and a notice that the code was modified is included with the above copyright notice. The Licensee may distribute binaries compiled with STLport (whether original or modified) without any royalties or restrictions. The Licensee may distribute original or modified STLport sources, provided that:

The conditions indicated in the above permission notice are met; The following copyright notices are retained when present, and conditions provided in accompanying permission notices are met : Copyright 1994 Hewlett-Packard Company Copyright 1996,97 Silicon Graphics Computer Systems, Inc.Copyright 1997 Moscow Center for SPARC Technology.

Index

A

Accounts and directories, creating 18
Adding
  Brightmail Scanner 77
  MySQL Connector/J to the CLASSPATH environment variable 81
Allowed and Blocked Senders Lists 9
AntiSpam Filters 8
AntiVirus Filters 10
Architecture overview 3

B

Blocked and Allowed Senders Lists 9
Brightmail Agent 5
Brightmail AntiSpam. See Symantec Brightmail AntiSpam.
Brightmail Client 5
Brightmail Conduit 11
Brightmail Control Center 5
  configuration 75
  configuring to use WebLogic 81
  hardware requirements 57
  installing 57
  installing on UNIX 60
  installing on Windows 67
  login 76
  operating system compatibility 58
  processes, services 73
  reinstalling on UNIX 67
  software requirements 58
  starting, automatic 73
  testing 75
  uninstalling 73
Brightmail Filter 33
Brightmail Filters 8
Brightmail JDBC Connection Pool 82
Brightmail Plug-in for Outlook. See Symantec Plug-in for Outlook.
Brightmail Quarantine. See Quarantine.
Brightmail Scanner 4
  adding 77
  hardware requirements for UNIX 15
  hardware requirements for Windows 43
  installing on UNIX 23
  installing on Windows 46
  modifying, repairing, removing on Windows 54
  removing on UNIX 31
  software requirements for UNIX 16
  software requirements for Windows 43
  starting from Control Center 78
  starting the first time on UNIX 30
  uninstalling on UNIX 31
  uninstalling on Windows 54
Brightmail Server 5
brightmail.war 86

C

Checking for port availability via TCP/IP 60
Checking software version 76
CLASSPATH 81
Compatibility, Quarantine/LDAP 59
Configuration Scenarios 87
Configuring
  automatic spam foldering 93
  Brightmail JDBC Connection Pool 82
  SMTP virtual server 50
  Spam Folder Agent 93
  Symantec Plug-in for Outlook 90
  Symantec Spam Folder Agent for Domino 95
Configuring Sendmail for the Brightmail Filter 33

via m4 41
via Sendmail Switch 35
via sendmail.cf 40
Connector/J API 81
Content filters 9
Control Center. See Brightmail Control Center.
Creating accounts and directories 18
Custom filters 9

D

Data Source (for WebLogic) 85
Deploying the brightmail.war 86
Directories and files 107

E

Email categories 6
Enabling
automatic spam foldering 105
Sendmail external filtering 17
Exchange
Spam Folder Agent 94

F

False positive submissions 11, 87
Features, new, in Version 6.0 2
Files and directories 107
Brightmail Control Center 134
Brightmail Scanner on UNIX 108
Brightmail Scanner on Windows 120
Filtering 6, 8
anti-spam 8
anti-virus 10
Blocked and Allowed Senders Lists 9
content filters 9
enabling Sendmail external 17
testing 79
Firewall conflict avoidance requirement 16
Foldering 11, 87
configuring 93
enabling 105

G

Group policies 6

H

Hardware requirements
Brightmail Control Center 57
Solaris, Brightmail Scanner 15
Windows, Brightmail Scanner 43

I

Install script, UNIX, accessing 61
Installation log, Brightmail Control Center 76
Installation sequence 12
Installer invocation methods 19, 62
Installing
Spam Folder Agent 94
Symantec Plug-in for Outlook 87
Symantec Spam Folder Agent for Domino 95
Installing Brightmail Control Center 57
installation log 76
installing MySQL Connector/J API 81
UNIX 60
Windows 67
Installing Brightmail Scanner
UNIX 23
Windows 46
Internet Explorer 59

J

JDBC Connection Pool 82
Junk mail. See Missed spam.

L

LDAP for Quarantine, compatibility 59
License file
UNIX 28
Windows 53
Licenses, for third party software 145
Linux
directories and files for Brightmail Control Center installation 61
directories and files for Brightmail Scanner installation 20
hardware requirements 16, 57
software requirements 16, 58
supported versions 16
Logging in and logging out 76

M

mailwall user 18
Message filtering, testing 79
Milter 33

Missed spam submissions 11, 87
Modifying Brightmail Scanner on Windows 54
MySQL, Connector/J API 81

N

Netscape browser 59
New features, Version 6.0 2

O

Operating system compatibility, Brightmail Control Center 58
Overview, Symantec Brightmail AntiSpam 1

P

Plug-ins and foldering 11, 87
Ports 60

Q

Quarantine 5, 11
  LDAP compatibility 59
  set up delivery of messages to Quarantine 80
  testing spam filtering to Quarantine 79

R

Red Hat Enterprise Linux, supported versions 16
Registering Symantec Brightmail AntiSpam
  UNIX 30
  Windows 52
Reinstalling Brightmail Control Center on UNIX 67
Removing Brightmail Scanner
  UNIX 31
  Windows 54
Repairing Brightmail Scanner, Windows 54

S

Scanner. See Brightmail Scanner.
Senders, lists of blocked and allowed senders 9
Sendmail
  configuring for Brightmail Filter 33
  configuring for Brightmail Filter with m4 41
  configuring for Brightmail Filter with sendmail.cf 40
  enabling external filtering 17
  mail filter API 33
  Milter 33
  Sendmail Switch 33
  Sendmail Switch, enable for Brightmail Filter 35
  verifying support 17
SMTP virtual server, configuring 50
Software compatibility, Quarantine/LDAP 59
Software requirements
  Brightmail Control Center 58
  Brightmail Scanner for UNIX 16
  Brightmail Scanner for Windows 43
  Symantec Plug-in for Outlook 89
Software version 76
Solaris
  directories and files for Brightmail Control Center installation 61
  directories and files for Brightmail Scanner installation 20
  hardware requirements 15, 57
  software requirements 16, 58
Spam
  false positive submissions 11, 87
  missed spam submissions 11, 87
Spam filtering, testing 79
Spam Folder Agent 94
  configuring 93
  enabling 105
  installing 94
Spam foldering 11, 87
  configuring 93
  enabling automatic 105
Starting
  Brightmail Control Center, automatic 73
  Brightmail Scanner from Control Center 78
  Brightmail Scanner the first time on UNIX 30
Submissions 11, 87
Symantec Brightmail AntiSpam
  architecture overview 3
  overview 1
  Registering on UNIX 30
  Registering on Windows 52
  Version 6.0 enhancements 2
Symantec Plug-in for Outlook
  administrator setup 89
  configuring 90
  end user experience 88
  setup 89
  software requirements 89
  Symantec menu items 88
Symantec Spam Folder Agent for Domino
  configuring 95

installing 95
uninstalling 103

T

TCP/IP Ports 60
Testing
anti-virus filtering 79
Brightmail Control Center 76
Brightmail Control Center with WebLogic 86
delivery of legitimate mail 78
spam filtering 79
spam filtering to Quarantine 79
spam filtering with subject line modification 79
Third party software
database, Web server 5
licenses 145

U

Uninstalling
Brightmail Control Center 73
Brightmail Scanner, Sendmail 31
Brightmail Scanner, Windows 54
Symantec Spam Folder Agent for Domino 103
UNIX
directories and files for Brightmail Control Center installation 61
directories and files for Brightmail Scanner installation 20
See also Linux, Solaris.
Upgrading
Brightmail Control Center 60
Brightmail Scanner for Sendmail 21
Brightmail Scanner for Windows 44
User mailwall 18

V

Verifying
Brightmail Control Center installation 76
Brightmail Scanner installation 53
normal delivery 78
Sendmail 8.12 support 17
spam filtering 79
spam filtering to Quarantine 79
Version 6.0 new features 2
Version checking 76
Virtual server, configuring SMTP virtual server 50

W

Web browser compatibility 59
WebLogic 81
Brightmail JDBC Connection Pool 82
brightmail.war 86
CLASSPATH 81
Data Source 85
testing Brightmail Control Center with WebLogic 86
What's New in Brightmail AntiSpam 2
Windows
hardware requirements 43, 57
software requirements 43, 58